Журнал Белорусского государственного университета. Право. 2019;1:72–80
Journal of the Belarusian State University. Law. 2019;1:72–80

УДК 343.4

ЗАРУБЕЖНЫЙ ОПЫТ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В. В. ВАБИЩЕВИЧ[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Рассмотрена зарубежная практика привлечения к уголовной ответственности лиц, совершивших преступные посягательства на персональные данные. Зарубежный опыт уголовно-правовой охраны персональных данных показывает, что введение уголовной ответственности за непосредственное нарушение законодательства о персональных данных является важным элементом предупреждения совершения преступлений в этой сфере, а также способствует эффективному исполнению законодательства о персональных данных. Рассмотрен опыт в данном вопросе России, Украины, Казахстана, Германии, Испании, Швеции, Швейцарии, Франции, Великобритании. Нормативно-правовая база в этих странах характеризуется конкретной регламентацией уголовной ответственности за посягательства на персональные данные. Отмечается наличие всех предпосылок и необходимости для надлежащей уголовно-правовой охраны персональных данных и дополнения Уголовного кодекса Республики Беларусь статьей, непосредственным объектом защиты которой станет установленный законодательством порядок оборота персональных данных.

Ключевые слова: персональные данные; защита информации; совершенствование законодательства; конституционные права; информационная безопасность; информационные технологии; посягательства на персональные данные.

FOREIGN EXPERIENCE OF CRIMINAL LAW PROTECTION OF PERSONAL DATA

V. V. VABISCHEVICH[a]

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*

The article deals with the foreign practice of bringing to criminal responsibility for criminal attacks on personal data. Foreign experience in criminal law protection of personal data shows that the introduction of criminal liability for direct violation of the legislation on personal data is an important element in the prevention of crimes in this area, as well as contributes to the effective implementation of legislation on personal data. Experience of the Russian Federation, Ukraine, Kazakhstan, Germany, Spain, Sweden, Switzerland, France, Great Britain is considered. The legal and regulatory framework in these countries is characterized by specific regulation of criminal liability for infringement of personal data. The author notes the presence of all the prerequisites and the need to establish appropriate criminal law protection of personal data and the addition of the Criminal code of the Republic of Belarus article, the direct object of protection of which will be established by the legislation of the order of circulation of personal data.

Keywords: personal data; information protection; improvement of legislation; constitutional rights; information security; information technology; attacks on personal data.

Образец цитирования:
Вабищевич ВВ. Зарубежный опыт уголовно-правовой охраны персональных данных. *Журнал Белорусского государственного университета. Право.* 2019;1:72–80.

For citation:
Vabischevich VV. Foreign experience of criminal law protection of personal data. *Journal of the Belarusian State University. Law.* 2019;1:72–80. Russian.

Автор:
Виталий Владимирович Вабищевич – аспирант кафедры уголовного права юридического факультета. Научный руководитель – кандидат юридических наук, доцент А. В. Шидловский.

Author:
Vitaly V. Vabischevich, postgraduate student at the department of criminal law, faculty of law.
r999m@mail.ru

Введение

С приходом компьютерной эры неизмеримо возросло значение защиты права на неприкосновенность частной жизни в информационной сфере. С одной стороны, в условиях современного развития цивилизации и повсеместного внедрения информационных технологий расширяется доступ людей к информации, что способствует осуществлению права индивида на свободу информации. С другой стороны, доступ физических лиц к базам данных усиливает риск вторжения в частную жизнь и нарушения права на ее неприкосновенность [1].

Пробел в исследовании проблем реализации норм права, обеспечивающих защиту персональных данных, может быть устранен путем введения эффективного правового регулирования отношений в сфере оборота персональных данных. Н. Г. Белгородцева отмечает, что нормативная правовая база и организация исследований проблем всех отраслей права, регулирующих отношения в области персональных данных, нуждаются в совершенствовании, корректировке многих имеющихся и разработке и введении новых научных постулатов и локальных актов. Проблемы могут быть решены в рамках серьезных научных исследований, на основе которых возможно создание отдельного закона, необходимость принятия которого продиктована срочным принятием мер, направленных на ужесточение законности по указанному направлению юриспруденции [2, с. 178].

Некоторые исследователи рассматривают правовую защиту персональных данных как договор граждан с государством, его учреждениями, банками, телефонными компаниями, интернет-магазинами и т. д. Подобный договор должен содержать ответственность каждого, кто решится выйти за его рамки и станет собирать иные сведения, считающиеся по закону частью того, что в английском языке именуется *privacy* и неточно переводится на русский, совмещая в себе понятия «личная жизнь» и «частное дело» [3].

В Республике Беларусь ведется работа над проектом закона о защите персональных данных, который был опубликован для общественного обсуждения[1]. Предметом регулирования законопроекта являются отношения, связанные со сбором, обработкой, распространением, предоставлением персональных данных, что осуществляется операторами с использованием и без использования средств автоматизации, если при этом обеспечивается поиск персональных данных и (или) доступ к таким персональным данным по определенным критериям (картотеки, списки, базы данных и др.).

В ст. 20 проекта закона установлено, что «лица, виновные в нарушении требований настоящего Закона, несут ответственность, предусмотренную законодательными актами»[2]. Представляется целесообразным наряду с принятием законопроекта выработать конкретные предложения по совершенствованию гражданского, административного, трудового и уголовного законодательства в части установления ответственности за посягательства на персональные данные, учитывая характер материальных и моральных последствий и способы совершения таких посягательств, а также субъект, совершивший посягательство, степень причиненного общественным отношениям вреда.

Реализация данных предложений будет надежной гарантией обеспечения прав и свобод граждан Республики Беларусь [4, с. 19].

Основная часть

Практика показывает, что посягательства на персональные данные могут причинить вред гражданам, субъектам хозяйствования, национальной безопасности страны. А персональные данные могут быть использованы в преступных целях, таких как мошенничество, недобросовестная конкуренция, киберпреследование, иные формы хищения, а также их хищение может стать способом совершения преступлений и являться необходимым действием в рамках приготовления к совершению любого преступления, в том числе убийства.

Действующие редакции статей Уголовного кодекса Республики Беларусь от 9 мая 1999 г. № 275-З (далее – УК Беларуси), связанные с посягательством на персональные данные, не претерпели существенных изменений с 1999 г., т. е. с момента принятия уголовного закона. Закономерно, что ранее вопрос об информационной безопасности личности, общества и государства не стоял так остро, а хищение персональных данных не рассматривалось как серьезное общественно опасное деяние, поскольку в меньшем количестве присутствовали информационные источники накопления персональных данных, а также технологии, позволяющие их похищать и использовать в преступных целях. В то же время законодатель регламентировал уголовно-правовую охрану некоторых видов информации, находящейся в ограниченном доступе, и обеспечил им надлежащую уголовно-правовую охрану. Например, разглашение тайны усыновления (удочерения) (ст. 177

[1]О персональных данных : проект закона Республики Беларусь [Электронный ресурс]. URL: http://forumpravo.by/files/proekt_zakona_o_personalnih_dannih.pdf (дата обращения: 01.09.2018).
[2]Там же.

УК Беларуси), разглашение врачебной тайны (ст. 178 УК Беларуси), разглашение коммерческой тайны (ст. 255 УК Беларуси), нарушение тайны голосования (ст. 192 УК Беларуси), нарушение тайны переписки, телефонных разговоров, телеграфных и иных сообщений (ст. 203 УК Беларуси), коммерческий шпионаж (ст. 254 УК Беларуси), умышленное разглашение государственной тайны (ст. 373 УК Беларуси), умышленное разглашение служебной тайны (ст. 375 УК Беларуси).

Уголовная ответственность наступает за незаконный сбор либо распространение информации о частной жизни (ст. 179 УК Беларуси), хищение путем использования компьютерной техники (ст. 212 УК Беларуси), несанкционированный доступ к компьютерной информации (ст. 349 УК Беларуси), изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившее существенный вред (ст. 350 УК Беларуси), умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (ст. 351 УК Беларуси), неправомерное завладение компьютерной информацией (ст. 352 УК Беларуси).

Если более детально рассмотреть перечисленные статьи, то они при определенных обстоятельствах могут быть связаны с хищением персональных данных, их разглашением. Однако статьи имеют свои специальные объекты, способы и средства совершения преступления. Объект защиты ст. 179 УК Беларуси вызывает много вопросов, поскольку имеет в виду сведения о частной жизни, которые касаются личной и семейной тайны другого лица. При этом законодательство Республики Беларусь не содержит определения личной и семейной тайны в отличие от банковской, финансовой, налоговой, коммерческой, адвокатской, врачебной, архивной и т. д.

Кроме того, вопрос определения личной и семейной тайны лежит в плоскости субъективного восприятия конкретно лица, так как информация об исполнении воинской обязанности для одного субъекта является тайной, а для другого не является. Более того, исполнение воинской обязанности – публичный священный долг гражданина перед государством, что также закреплено в ст. 57 Конституции Республики Беларусь. В связи с этим возникает вопрос о правильном определении объекта посягательств по ст. 179 УК Беларуси и квалификации тех либо иных деяний.

Задача уголовного закона состоит в охране человека, его прав и свобод, собственности, прав юридических лиц, природной среды, общественных и государственных интересов, конституционного строя Республики Беларусь. Уголовный закон способствует предупреждению преступных посягательств, воспитанию граждан в духе соблюдения законодательства. Право гражданина на защиту от незаконного вмешательства в его личную жизнь закреплено в Конституции Республики Беларусь, что подтверждает значимость надлежащей охраны этого права, в том числе уголовно-правовой. Кроме этого, М. И. Проскурякова отмечает, что охрана персональных данных также связана с такими конституционными правами человека, как право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, право на неприкосновенность жилища, а вышеперечисленные права образуют конституционно-правовые рамки защиты персональных данных [5, с. 15].

Таким образом, по нашему мнению, не вызывает сомнений целесообразность выработки предложений, направленных на криминализацию конкретных деяний путем введения в УК Беларуси статьи, непосредственным объектом защиты которой станет установленный законодательством порядок совершения определенных действий с персональными данными (обработка, сбор, трансграничная передача, хранение, обезличивание, разглашение и т. д.).

Рассмотрим законодательное регулирование охраны персональных данных, криминализацию посягательств на них в ряде зарубежных государств. В целом подходы разных стран к вопросам защиты неприкосновенности частной жизни и индивидуальных свобод имеют много общего. Среди ключевых элементов системы охраны персональных данных можно назвать следующие: ограничение объема запрашиваемых персональных данных; создание механизмов, позволяющих индивидууму узнавать о наличии в обращении и о содержании его персональных данных; указание реквизитов лиц, несущих ответственность за соблюдение соответствующих правил и решений, касающихся неприкосновенности частной жизни. При этом существуют различия в национальных подходах, которые касаются таких аспектов, как лицензионные требования и механизмы контроля в форме специальных органов надзора («инспекций по проверке персональных данных»). В качестве примеров можно указать различия в категоризации данных, не подлежащих разглашению [3].

Республика Казахстан первой из стран Евразийского экономического союза регламентировала уголовное наказание за непосредственное нарушение законодательства о персональных данных. После принятия Закона от 21 мая 2013 г. № 94-V «О персональных данных и их защите» в ст. 147 Уголовного кодекса Республики Казахстан от 3 июля 2014 г. № 226-V (далее – УК Казахстана) были внесены изменения, согласно которым преступными стали признаваться деяния, связанные с несоблюдение мер по защите персональных данных лицом, на которое

возложена обязанность принятия таких мер, если эти деяния причинили существенный вред правам и законным интересам лиц. При этом под существенным вредом понимается в том числе нарушение конституционных прав и свобод человека и гражданина. К иным уголовно наказуемым деяниям относится причинение существенного вреда правам и законным интересам лица в результате незаконных сбора и (или) обработки персональных данных. Квалифицирующими признаками являются:

- совершение указанных деяний с использованием служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сети телекоммуникаций, либо в целях извлечения выгод и получения преимуществ для себя или других лиц или организаций;
- распространение сведений в публичном выступлении, прилюдно демонстрирующемся произведении, в средствах массовой информации или с использованием сетей телекоммуникаций. За совершение данного преступления предусмотрено уголовное наказание в виде лишения свободы на срок до семи лет[3].

Украина 1 июня 2010 г. № 2297-VI приняла Закон «О защите персональных данных», ратифицировала конвенцию Совета Европы о защите персональных данных и дополнительный протокол к конвенции о защите лиц, связанный с автоматизированной обработкой персональных данных относительно органов надзора и трансграничных потоков данных, чем приблизила украинское законодательство к европейским стандартам защиты информации[4].

Украинский законодатель также разрабатывал проект закона «О внесении изменений в некоторые законодательные акты Украины относительно нарушения законодательства о защите персональных данных». Цель законопроекта заключалась в том, чтобы установить административную и уголовную ответственность за нарушение требований по защите персональных данных, что, в свою очередь, должно было усилить защиту права человека, закрепленного в ст. 32 Конституции Украины от 28 июня 1996 г. № 254 к/96-ВР, согласно которой не допускается сбор, хранение, использование и распространение конфиденциальной информации о лице без его согласия, кроме случаев, определенных законом, и только в интересах национальной безопасности, экономического благосостояния[5].

Предлагалось изложить ст. 182 Уголовного кодекса Украины от 5 апреля 2001 г. № 2341-III (далее – УК Украины) в новой редакции, а также дополнить уголовный закон статьями 181-1, 182-2, установив уголовную ответственность:

- за незаконный сбор, регистрацию, накопление, хранение, адаптирование, изменение, обновление, использование, уничтожение или распространение (включая само распространение, а также реализацию, передачу) конфиденциальной информации о личности, в том числе в публичном выступлении, прилюдно демонстрируемом произведении или в средствах массовой информации, а также ее передачу третьим лицам с нарушением требований закона;
- нарушение установленных законом требований относительно защиты информации о лице, что привело к несанкционированному распространению или искажению этой информации и причинило значительный ущерб лицу;
- умышленное предоставление владельцем, распорядителем базы персональных данных или уполномоченным лицом доступа к информации о лице или его умышленная передача третьим лицам с нарушением закона, что привело к несанкционированному распространению или искажению этой информации и причинило значительный ущерб лицу.

Однако вышеперечисленные предложения поддержаны не были, а изменения были внесены только в ст. 182 УК Украины, согласно которой уголовная ответственность устанавливается за незаконное собирание, хранение, использование, уничтожение, распространение конфиденциальной информации о лице или незаконное изменение такой информации, кроме случаев, предусмотренных другими статьями кодекса, а также совершение тех же действий повторно или если они причинили существенный вред охраняемым законом правам, свободам и интересам лица. Под существенным вредом, если он заключается в причинении материальных убытков, в указанной статье понимается такой материальный ущерб, который в сто и более раз превышает необлагаемый минимум доходов граждан.

Как видно, в УК Украины, в отличие от УК Казахстана, конкретизируются определение существенного вреда, а также категоризация видов неправомерных действий с персональными данными (собирание, хранение, уничтожение и т. д.).

В целом в законодательстве государств – участников СНГ персональные данные трактуются посредством информации, которая идентифицирована или может быть идентифицирована с конкретным физическим лицом [6, с. 19].

[3]Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31575252#pos=1885;-100 (дата обращения: 16.02.2018).

[4]Защита персональных данных: придется отвечать [Электронный ресурс]. URL: http://averba.com.ua/advokat-yuridicheskie-yslygi-dnepropetrovsk/zashhita-personalnyx-dannyx-pridetsya-otvechat.html (дата обращения: 16.02.2018).

[5]Законодательство Украины [Электронный ресурс]. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JF5OB00A.html (дата обращения: 16.02.2018).

В Европейском союзе принято значительное число актов, регулирующих порядок обработки персональных данных и их защиту. В связи с этим внутреннее законодательство стран – участниц ЕС детально регламентирует ответственность за нарушение законодательства о персональных данных.

В Федеративной Республике Германии такая ответственность регулируется Законом от 14 января 2003 г. «О защите данных», который был принят в целях реализации Директивы Европейского союза от 24 октября 1995 г. № 95/46/ЕС. Согласно ст. 44 указанного закона преступными признаются умышленные либо неосторожные деяния лиц, которые:

• без разрешения собирают или обрабатывают персональные данные, доступ к которым ограничен, хранят персональные данные, которые находятся в ограниченном доступе и не могут быть получены с помощью установленной автоматизированной процедуры, извлекают личные данные, которые не являются общедоступными или получают такие данные для себя или других с помощью операций автоматической обработки;

• получают персональные данные посредством предоставления неверных сведений (фактически путем обмана);

• получили в установленном порядке персональные данные для определенных целей, однако обрабатывают или используют эти персональные данные в других целях. Указанное правило распространяется также на лиц, которые при исполнении своих профессиональных или служебных обязанностей должны были обеспечить надлежащее хранение персональных данных и их целевое использование, а также в случае, когда персональные данные были собраны или сохранены для научных исследований;

• обрабатывают и используют персональные данные для целей рекламного или маркетингового исследования в случае, когда субъект, которому принадлежат персональные данные, заранее возразил против этого;

• нарушили, в том числе при ведении бизнеса, порядок обезличивания персональных данных и передачи их в анонимной форме, что повлекло возникновение возможности идентифицировать конкретных физических лиц;

• не сообщили о незаконном доступе к определенным персональным данным (например, к данным о банковских счетах) в случае, когда такая обязанность на них лежала.

При этом к уголовной ответственности могут быть привлечены лица, совершившие указанные действия, только в случае причинения вреда общественным отношениям либо если лица совершили действия из корыстных побуждений, а также при наличии соответствующей жалобы, которая может подаваться федеральным уполномоченным по защите данных и свободе информации и контролирующими органами. Максимальный срок тюремного заключения за совершение перечисленных преступлений составляет два года[6].

Конкретные составы преступлений, касающиеся посягательств на персональные данные, содержатся и в Уголовном кодексе Федеративной Республики Германии от 14 января 2008 г. (далее – УК ФРГ). Так, в ст. 169 УК ФРГ регламентируется ответственность за сокрытие или предоставление ложных сведений о гражданском состоянии другого лица учреждению, ответственному за ведение книги записей гражданского состояния. Данные о гражданском состоянии относятся к персональным. Как видно, немецкий законодатель устанавливает ответственность за предоставление ложных персональных данных уполномоченному органу либо за их сокрытие. Согласно ст. 201 УК ФРГ наказывается субъект, который незаконно подслушивает конфиденциальную информацию конкретного лица и предоставляет доступ к ней другим лицам. Такие деяния признаются преступными, если могут нанести вред законным интересам конкретного лица. При этом до пяти лет лишения свободы вменяется тому, кто, будучи должностным лицом или лицом, специально уполномоченным на выполнение публичной службы, нарушает конфиденциальность информации о другом лице[7].

Согласно ст. 202а УК ФРГ преступником признается тот, кто противоправно получает или предоставляет другому лицу не предназначенные для этого сведения, которые защищены от незаконного доступа к ним, посредством использования электронных, магнитных или иных средств. В ст. 203а УК ФРГ достаточно детально регулируются общественно опасные деяния, связанные с нарушением тайны частной жизни. Такие деяния зависят от рода деятельности распространителя информации (врач, психолог, опекун, адвокат, аудитор, консультант по вопросам брака, семьи, воспитания или проблемам молодежи, специалист по вопросам, связанным с беременностью, социальный работник, педагог, представитель частных страховых организаций и т. д.). Также наказывается тот, кто раскрывает чужую тайну, касающуюся личной жизни, которая была ему доверена или стала известной ему, как должностному лицу, специально уполномоченному на выполнение обязанностей публичной службы, как члену комитета по расследованию или лицу, которое официально на основании закона обязано ответственно выполнять свой долг

[6]Federal Data Protection in the version promulgated on 14 January 2003 [Electronic resource]. URL: http://www.wipo.int/edocs/lexdocs/laws/en/de/de202en.pdf (date of access: 16.02.2018).

[7]Уголовный кодекс ФРГ [Электронный ресурс] // Российский правовой портал: Библиотека Пашкова. URL: http://constitutions.ru/?p=5854&page4 (дата обращения: 16.02.2018).

по сохранению тайны при осуществлении научно-исследовательских работ и т. д. Стоит отметить, что к ответственности привлекаются преступники и в случае нарушения тайны лица после его смерти. Квалифицирующими признаками является цель нарушения тайны другого лица, а именно получение вознаграждения, личной выгоды, обогащение другого лица или нанесение вреда другому лицу.

Немецкий опыт уголовно-правовой охраны личной информации граждан основан на детальном и достаточно жестком европейском регулировании порядка обращения персональных данных, их широком определении, что подчеркивает важность и значимость недопущения нарушений при сборе персональной информации, ее хранении, передаче, разглашении и использовании.

В Испании действует Закон «О защите данных» (*Ley Orgánica* 15/1999), за серьезные нарушения которого правонарушители могут быть привлечены к штрафу в размере до 757 000 долл. США. При этом штрафные санкции применяются в зависимости от характера нарушенного права, количества операций по обработке персональных данных, полученной прибыли, умышленного характера правонарушения, ущерба, причиненного субъектам данных и третьим лицам, и любых других последствий, имеющих отношение к определению степени незаконности и виновности конкретного правонарушителя.

В дополнение к административным штрафам, которые могут быть наложены в соответствии с законом, в Уголовном кодексе Испании (далее – УК Испании) также содержатся составы преступлений, связанные с нарушениями неприкосновенности частной жизни, включая обработку персональных данных. К таким преступлениям относятся:

• сбор персональных данных, доступ к которым ограничен, путем незаконного перехвата электронных сообщений, файлов или других коммуникационных сигналов;

• несанкционированное присвоение, использование или изменение конфиденциальной информации или персональных данных, хранящихся в государственных или частных электронных файлах, что приносит ущерб субъекту данных или третьему лицу;

• передача данных, незаконно полученных контролером или обработчиком персональных данных;

• сбор и передача персональных данных, раскрывающих идеологию, религию, убеждения, состояния здоровья, расовое происхождение или сексуальную ориентацию субъекта, а также в том случае, если жертва является несовершеннолетним лицом или инвалидом, либо в случае, когда вышеупомянутые действия совершены в целях получения прибыли[8].

УК Испании конкретизирует виды «чувствительных» персональных данных, указывает на вид потерпевшего (несовершеннолетнее лицо либо инвалид) как на квалифицирующий признак, а также предусматривает такой способ совершения преступления, как перехват данных.

В соответствии с разделом 41 Закона Франции от 6 января 1978 г. № 78-17 «О защите данных» к уголовной ответственности на срок от шести месяцев до пяти лет может быть привлечено любое лицо:

• за автоматическую обработку персональных данных или получившее такую обработку без получения официальных разрешений (постановление, принятое после получения мотивированного заключения Национальной комиссии по обработке данных и свободе либо на основании Указа о благоприятном мнении Совета безопасности) или не представившее заявление в Национальную комиссию по обработке данных и свободе о получении разрешения на автоматическую обработку персональных данных;

• сбор персональных данных любыми мошенническими, нечестными и незаконными способами, а также действия лиц, которые без разрешения обрабатывают персональные данные любого физического лица, нарушают срок хранения персональных данных, не предпринимают надлежащих мер предосторожности для защиты данных и, в частности, для предотвращения их искажения, повреждения или несанкционированного разглашения, без разрешения записывают либо хранят на программных средствах персональные данные прямо или косвенно отражающие расовое происхождение, политические, философские или религиозные взгляды, членство в профсоюзах;

• сбор, хранение, передачу или любую другую форму обработки персональных данных, их разглашение, что может повлечь за собой ухудшение репутации или нарушение частной жизни физического лица. К ответственности за данное преступление привлекается и тот, кто неосмотрительно или небрежно разглашает или разрешает разглашать персональные данные[9].

УК Франции устанавливает ответственность за нецелевое использование персональных данных, предусматривает форму неумышленной вины за совершение посягательств на персональные данные. В качестве последствий посягательств указывается ухудшение репутации потерпевшего.

В Великобритании отсутствует единый кодифицированный уголовный закон, а статьи об уголовной ответственности за те либо иные преступления содержатся в специальных актах, регулирующих

[8]Spanish Data Protection Agency [Electronic resource]. URL: https://loc.gov/law/help/online-privacy-law/spain.php (date of access: 16.02.2018).

[9]Act French 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties [Electronic resource]. URL: https://ssi.ens.fr/textes/a78-17-text.html (date of access: 16.02.2018).

определенные отрасли правоотношений. Практика британских судов свидетельствует о жестком подходе при привлечении к ответственности преступников за посягательства на персональные данные. К ответственности даже привлекаются, например, журналисты за то, что распространяют сведения, полученные на вполне законных основаниях [7].

Регулирование обработки персональных данных в Великобритании осуществляется Законом «О защите персональных данных» (Data Protection Act 1998)[10], который содержит ряд составов уголовных преступлений в этой сфере. В силу ст. 56 указанного закона преступлением признается требование у человека информации, касающейся его убеждений и взглядов, при приеме на работу либо при оказании услуги, выполнении работы. Уголовная ответственность наступает за незаконное разглашение персональных данных, если эти действия причинили или могли причинить существенный вред человеку, персональные данные которого разглашены, или причинили существенный вред его правам и свободам[11].

Важно отметить, что в законе предусмотрены конкретные исключения, когда, например, обработка персональных данных в целях обеспечения национальной безопасности освобождается от всех принципов защиты. Данные, обрабатываемые для предупреждения или обнаружения преступлений, задержания или судебного преследования правонарушителей, для оценки или сбора налогов, также не подпадают под действие закона о защите данных. В Великобритании рассматриваются предложения об ужесточении ответственности за посягательства на персональные данные. Некоторые специалисты отмечают, что в Великобритании предусматривается наказание в двух случаях: при нарушении установленного порядка защиты персональных данных и в случае их утечки. Второе нарушение рассматривается как более тяжкое. Для сравнения в США только утечка, утрата и разглашение персональных данных влечет за собой наказание, а за неправильное хранение не предусмотрена уголовная или административная ответственность[12].

Одним из видов хищения персональных данных и их использования в целях причинения вреда отдельным гражданам является киберпреследование. На практике зафиксировано достаточное количество случаев, когда злоумышленник похищает персональную информацию и в дальнейшем использует ее для нарушения спокойствия жертвы.

В соответствии со ст. 179 Уголовного кодекса Швейцарии от 21 декабря 1937 г. к уголовной ответственности привлекается тот, кто незаконно получает из различных баз данных особо защищаемые личные данные или сведения о личности, которые не являются общедоступными. Кроме этого, преступлением признается использование сведений из телефонного справочника для беспокойства другого лица. Уголовные дела за совершение этих деяний возбуждаются по жалобе потерпевшего, т. е. являются делами частного обвинения.

В Швеции действует Закон от 29 апреля 1998 г. «О защите данных», который предусматривает уголовную ответственность за посягательства на персональные данные и имеет при этом отличия от законодательств других стран ЕС. Например, в соответствии со ст. 49 закона лишением свободы от шести месяцев до двух лет наказывается лицо, которое намеренно или по небрежности не в установленном порядке совершает следующие деяния:

• обрабатывает персональные данные благодаря своему служебному положению и профессиональным умениям (работники некоммерческих предприятий, организаций здравоохранения, социального обеспечения, научных и статистических исследований и т. д.). При этом заинтересованность общества в научно-исследовательской работе, в процессе которой обрабатываются персональные данные, должна быть значительно выше, чем риск нарушения личной неприкосновенности лиц, данные которых используются. В некоторых случаях необходимо получение разрешения об использовании персональных данных в Комитете по научной этике;

• обрабатывает личные данные о правонарушителях, связанные с преступлениями, судебными решениями по уголовным делам, мерами уголовно-процессуального принуждения или лишения свободы;

• передает персональные данные иностранным государствам, не имеющим достаточный уровень защиты персональных данных. Адекватность уровня защиты оценивается с учетом всех обстоятельств, связанных с передачей. Особое внимание уделяется характеру данных, цели и продолжительности обработки, стране происхождения, стране конечного назначения и правилам, которые существуют для обработки данных в третьей стране. В любом случае допускается передача данных только в те государства, которые присоединились к Конвенции Совета Европы «О защите

[10]Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998 [Electronic resource]. URL: https://gov.uk/government/uploads/system/uploads/attachmentdata/file/422792/ico-guidance-money-penalties-2015.pdf (date of access: 16.02.2018).

[11]Законодательство Великобритании о преступлениях в сфере компьютерной информации [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/zakonodatelstvo-velikobritanii-o-prestupleniyah-v-sfere-kompyuternoy-informatsii (дата обращения: 16.02.2018).

[12]В Великобритании ужесточают наказание за нарушение закона о защите данных (PDA) [Электронный ресурс]. URL: https://infowatch.ru/analytics/leaks_monitoring/192 (дата обращения: 16.02.2018).

физических лиц при автоматизированной обработке персональных данных» (Республика Беларусь к ней не присоединилась)[15].

Анализ уголовного законодательства зарубежных стран показывает, что, как правило, уголовная ответственность устанавливается:

• за несоблюдение мер по защите персональных данных лицом, на которое возложена обязанность принятия таких мер, если это деяние причинило существенный вред правам и законным интересам лиц;

• хищение персональных данных с использованием технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам;

• обработку и использование персональных данных в целях проведения рекламного или маркетингового исследования в случае, когда субъект, которому принадлежат персональные данные, заранее возразил против этого;

• нарушение, в том числе при ведении бизнеса, порядка обезличивания персональных данных и их передачи в анонимной форме, что повлекло за собой возможность идентификации конкретных физических лиц. Некоторые авторы отмечают, что сегодня по непонятным причинам действия по обезличиванию персональных данных вынесены за рамки правового регулирования и переданы в полное распоряжение операторам персональных данных. Сложность возникает в том, что, предоставляя операторам возможность самостоятельно выбирать методы и способы защиты обезличенной информации, законодатель дистанцировался от закрепления процедуры ее обезличивания, что в том числе влечет за собой сложности при привлечении лиц к ответственности за нарушение порядка обезличивания персональных данных [8, с. 15–16];

• несообщение обязанными лицами о незаконном доступе к определенным персональным данным (например, к данным о банковских счетах);

• сбор и передачу персональных данных, раскрывающих идеологию, религию, убеждения, здоровье, расовое происхождение или сексуальную ориентацию субъекта, или если жертва является несовершеннолетним лицом или инвалидом, либо в случае, когда вышеупомянутые действия совершены в целях получения прибыли;

• получение персональных данных любыми мошенническими, нечестными и незаконными средствами;

• нарушение срока хранения персональных данных и непринятие надлежащих мер предосторожности для их защиты и, в частности, для предотвращения их искажения, повреждения или несанкционированного разглашения;

• передачу в неустановленном порядке персональных данных иностранным государствам, не имеющим достаточный уровень защиты персональных данных.

Заключение

На основании проведенного анализа необходимо отметить, что Республика Беларусь движется в правильном направлении, находясь на пути принятия специального законодательства в сфере оборота и защиты персональных данных. Надлежащая регламентация вопросов, связанных с определением персональных данных, принципов их обработки, порядка сбора, хранения, передачи, обезличивания, разглашения, а также связанных с регулированием прав и обязанностей субъектов персональных данных, в том числе операторов, общих положений об ответственности за нарушение законодательства о персональных данных, компетенции государственных органов является очень важным элементом сохранения баланса между развитием информационного общества, цифровой экономики и охраной конституционных прав граждан и национальной безопасности.

Зарубежный опыт уголовно-правовой охраны, в том числе развитых стран, в которых, как правило, степень криминализации тех либо иных деяний, а также уголовная ответственность за их совершение значительно ниже, показывает, что введение уголовной ответственности за непосредственное нарушение законодательства о персональных данных является важным элементом предупреждения совершения преступлений в этой сфере, а также способствует эффективному исполнению законодательства о персональных данных.

Нормативно-правовая база в Казахстане, Германии, Швеции, Испании, Франции, Швейцарии, Великобритании характеризуется конкретной регламентацией уголовной ответственности за посягательства на персональные данные. Объективная сторона таких посягательств, как правило, заключается в незаконном обороте персональных данных, непринятии мер по надлежащей их охране, раскрытии «чувствительных» персональных данных. Составы преступлений имеют материальный характер, заключающийся в наличии ущерба, в том числе морального вреда. Отягчающими вину обстоятельствами, наряду с общими, являются повторность, использование властных полномочий, специализированных автоматических систем. Отдельным видом

[13]Personal Data Act (1998:204) issued 29 April 1998 [Electronic resource]. URL: http://legislationline.org/download/action/download/id/1296/file/5d5116c153d4b0fa477093f138ac.pdf (date of access: 16.02.2018).

преступления является передача персональных данных в другие страны, в которых не установлено надлежащее правовое регулирование и правовая охрана персональных данных.

Таким образом, наряду с разработкой закона Республики Беларусь о защите персональных данных предлагается установить надлежащую уголовно-правовую охрану персональных данных, дополнив УК Беларуси статьей, непосредственным объектом защиты которой станет установленный законодательством порядок оборота персональных данных. Необходимо также определить субъект, который совершает такие преступления, способы и средства посягательств на персональные данные, регламентировать конкретные признаки и критерии определения персональных данных как предмета уголовно-правовой охраны, установить иные обстоятельства, влияющие на квалификацию преступных деяний.

Библиографические ссылки

1. Пискунова ЮВ. К вопросу о правовом регулировании общественных отношений при сборе и обработке информации о частной жизни гражданина. *Вестник Академии*. 2010;3:93–94.
2. Белгородцева НГ. Об особенностях правового регулирования в области защиты информации персонального характера. *Право и образование*. 2011;5:177–180.
3. Волчинская ЕК. *Защита персональных данных: опыт правового регулирования*. Москва: Галерия; 2001.
4. Абламейко МС. Правовое регулирование персональных данных с учетом введения ID-карт и биометрических паспортов. *Журнал Белорусского государственного университета. Право.* 2018;1:14–20.
5. Проскурякова МИ. Конституционно-правовые рамки защиты персональных данных в России. *Вестник Санкт-Петербургского университета. Право.* 2016;2:12–27.
6. Валюшко-Орса НВ. Сущностно-содержательные аспекты персональных данных в Республике Беларусь. *Журнал Белорусского государственного университета. Право.* 2017;2:17–23.
7. Перова НА. Ограничения свободы слова в целях предотвращения разглашения личной и государственной тайны в праве США и Великобритании. *Право и управление. XXI век.* 2012;1:93–99.
8. Бабичев ДС. Некоторые проблемы практического применения законодательства РФ о персональных данных. *Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики.* 2010;2:15–17.

References

1. Piskunova UV. [To the question of legal regulation of public relations in the collection and processing of information about the private life of a citizen]. *Vestnik Akademii.* 2010;3:93–94. Russian.
2. Belgorodtseva NG. [About features of legal regulation in the field of protection of information of personal character]. *Pravo i obrazovanie.* 2011;5:177–180. Russian.
3. Volchinskaya EK. *Zashchita personal'nykh dannykh: opyt pravovogo regulirovaniya* [Personal data protection: experience of legal regulation]. Moscow: Galeriya; 2001. 223 p. Russian.
4. Ablameyko MS. Legal regulation of personal data taking into account the use of ID-cards and biometric passports. *Journal of Belarusian State University. Law.* 2018;1:14–20. Russian.
5. Proskuryakova MI. [Constitutional and legal framework of personal data protection in Russia]. *Vestnik Sankt-Peterburgskogo universiteta. Pravo.* 2016;2:12–27. Russian.
6. Valiushko-Orsa NV. Essentially-content aspects of personal data in the Republic of Belarus. *Journal of the Belarusian State University. Law.* 2017;2:17–23. Russian.
7. Perova NA. [Restrictions on freedom of speech in order to prevent disclosure of personal and state secrets in the US and UK law]. *Journal of Law and Administration.* 2012;1:93–99. Russian.
8. Babichev DS. [Some problems of practical application of the legislation of the Russian Federation on personal data]. *Historical, philosophical, political and legal sciences, cultural studies and art history. Theory and practice.* 2010;2:15–17. Russian.

Статья поступила в редколлегию 04.12.2018.
Received by editorial board 04.12.2018.