По мнению В.В. Марчука, нормативная обособленность не является обязательным признаком правового института, однако, рассматривая институт «квалификации преступлений», автор отмечает, что законодательное обособление всегда способствует реализации задачи по систематизации норм института и полезно в организационно-практическом аспекте. Аналогичный подход наблюдается в работах Л.Л. Кругликова и Л.Е. Смирнова. Исследуя проблемы унификации в уголовном праве, ученые отмечают, что обособление в самостоятельное структурное подразделение нормативного акта правового института выступает завершающим этапом его формирования.

Обособление рассматриваемых институтов в различных главах уголовного кодекса нашло отражение в законодательстве большинства стран СНГ. В качестве примера можно назвать уголовные законы Азербайджана (гл. 11, 12), Армении (гл. 11, 12), Кыргызстана (гл. 11, 12), Таджикистана (гл. 11, 12), Туркменистана (гл. 10, 11), Узбекистана (гл. 12, 13). Часть уголовных законов стран СНГ и вовсе «распределяет» рассматриваемые институты по еще более крупным структурным единицам нормативного правового акта – разделам (например, УК Украины (разд. 9, 12)).

Таким образом, полагаем необходимым выделение норм, регулирующих освобождение от наказания, в отдельную главу УК Республики Беларусь. Нормативная обособленность может являться дополнительным разграничительным барьером между освобождением от наказания и смежным для него институтом – освобождением от уголовной ответственности. Законодательное выделение системы связанных норм, которым присуща однородность регулируемых отношений, позволяет не только достигнуть стройности, четкости и логичности уголовного закона, систематизации и структуризации норм УК, унифицирования подхода к регламентации сходных отношений, но и в перспективе позволит повысить уровень внутренней структуры института освобождения от уголовного наказания, а правоприменителям обеспечит лучшее понимание его правовой природы, будет способствовать правильному и единообразному применению уголовного закона.

УДК 343.2/.7

В.В. Вабищевич

ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В СФЕРЕ НЕЗАКОННОГО ИСПОЛЬЗОВАНИЯ И ОБРАЩЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Фишинг, смишинг, фарминг, спуфинг, кибер-преследование, кардинг, кража личности, социальный инжиниринг – это лишь небольшая часть вошедших в оперативный оборот формулировок, обозначающих совершение общественно опасных деяний, связанных с хищением, незаконным оборотом и использованием персональных данных для достижения негативного результата, направленного на причинение вреда отдельным гражданам, обществу и государству. Сегодня в Беларуси отсутствует системный нормативный правовой акт, регулирующий использование и обработку персональных данных, несмотря на наличие модельного закона «О персональных данных» для стран – участниц СНГ. Республика Беларусь также не ратифицировала Конвенцию о защите физических лиц в отношении автоматизированной обработки данных личного характера.

Следует обратить внимание на отсутствие конкретных составов в Уголовном кодексе Республики Беларусь, предусматривающих ответственность за нарушение законодательства о персональных данных, что ограничивает применение мер уголовной ответственности в этой сфере.

Действующие редакции статей уголовного закона, так или иначе связанные с посягательством на персональные данные, не претерпели существенных изменений с 1999 г., т. е. с момента принятия УК. Закономерно, что 18 лет назад вопрос информационной безопасности личности, общества и государства не стоял так остро, а хищение персональных данных не рассматривалось как серьезное общественно опасное деяние, так как отсутствовали в таком количестве информационные источники накопления персональных данных, а также технологии, позволяющие их похищать и использовать в преступных целях.

Стоит отметить, что в настоящее время ведется обсуждение принятия закона о персональных данных, защиту которых в том числе обеспечит криминализация конкретных деяний, связанных с нарушением законодательства о персональных данных. Введение в УК отдельных составов упростит работу правоохранительных органов, станет качественной превентивной мерой, в том числе в отношении хакеров, которые похищают персональные данные «ради интереса» и удовлетворения собственных профессиональных амбиций.

Уголовная ответственность за сам факт хищения персональных данных предусмотрена в Европейском союзе, США, Канаде, Японии, Китае и во многих других странах мира. Некоторыми зарубежными исследователями хищение персональных данных определено, как мошенничество или иное незаконное действие, когда персональные данные существующего лица используются в качестве основного инструмента для совершения иных преступлений.

Согласно п. 1028 (a) (7) Закона США «О краже персональных данных и сдерживании присвоения» наказывается лицо, которое осознанно передает или использует без законного на то права средства идентификации другого лица для совершения или содействия, или подстрекательства к незаконной деятельности. В США кража персональных данных, их незаконный оборот либо использование является самостоятельным и специальным объектом соответствующего уголовного преступления, что вызвано, например, значительным количеством полученных американским Центром приема сообщений об интернет-преступлениях (около 150 000), переданных правоохранительным органам, из которых 14 % составляла кража персональных данных.

В Великобритании ежечасно совершается около 1 000 кибератак, часть из которых направлена на хищение персональных данных. Сам факт хищения персональных данных уже является основанием для потери организацией доверия и репутации со стороны клиентов. Так, одна из крупных зарубежных компаний в результате кражи у нее персональных данных, в том числе гражданином Беларуси, закрылась. В 2007 г. двое белорусов создали «криминальный стартап», основанный на кра-

же «личностей». Злоумышленники находили персональную информацию о жертве и использовали ее в целях легализации транзакций через соответствующие банки, а в 2009 г. в США белоруса признали причастным «к самому крупному хищению персональной информации за всю историю страны», что могло грозить для него пожизненным заключением.

В настоящая время всемирно известная социальная сеть Facebook имеет около 83 млн фальшивых аккаунтов, значительная часть из которых используется для хищения персональных данных.

В Литве уделяется огромное внимание борьбе с преступностью в сфере хищения персональных данных. Так, представитель Государственной инспекции защиты данных Вильнюса Дангуоле Моркунене отметила постоянно растущий объем жалоб на виртуальных мошенников, ворующих персональные данные в личных целях. Хищение персональных данных используется и в более тяжких преступлениях. По словам эксперта по вопросам кибербезопасности и нормативной правовой базы в сфере IT Виктора Дуброва, имеется информация о трех убийствах граждан, персональные данные которых были похищены и представлены как неугодные потенциальным преступникам на известном украинском портале «Миротворец».

Недавно в Китае за кражу персональных данных были задержаны почти пять тысяч человек, которые являются фигурантами 1,8 тыс. уголовных дел, возбужденных по фактам похищения и несанкционированного использования данных.

Необходимость в надлежащей защите персональных данных на национальном уровне подтверждается мерами, принятыми Российской Федерацией, в частности принятием Закона «О локализации баз персональных данных». После принятия указанного Закона соответствующие службы провели порядка 2 500 проверок и выявили 56 правонарушений, из-за которых под угрозой неправомерного использования находилась личная информация более чем 90 млн россиян. Кроме того, в России обсуждается вопрос о введении в уголовное законодательство отдельной статьи за хищение банковских паролей. Такое предложение было изложено в заключении Национального совета финансового рынка, так как становление информационного общества связано с ростом посягательств на собственность посредством использования персональных данных клиентов банка.

Как отмечает руководитель представительства компании – разработчика антивирусных программ ESET в России и СНГ Денис Матеев, у граждан Беларуси и России после опасения кражи денег в интернете на втором месте стоит боязнь потерять личные данные, например переписку. Специалист утверждает, что в ближайшем будущем «в бизнес превратится все, что связано с кражей персональных данных».

По мнению автора, в настоящее время сформировались все криминологические аспекты и необходимость в уголовно-правовой охране персональных данных. Уголовный кодекс содержит ряд статей, предусматривающих ответственность за преступления, объект которых тесно связан с персональными данными. Однако за хищение персональных данных, нарушение порядка их оборота, хранения и защиты уголовная ответственность не предусмотрена. Не криминализирована и утечка персональных данных по неосторожной вине соответствующих должностных лиц, связанная с халатной обработкой и хранением персональных данных, повсеместным использованием контрафактного программного обеспечения и в целом с отсутствием экономических, законодательных и социально-психологических условий для соблюдения законности в сфере оборота персональных данных.

Таким образом, наряду с рассмотрением вопроса о принятии нормативного правового акта, направленного на установление порядка обращения с персональными данными, видится целесообразным разработать специальные составы, имеющие непосредственный уголовно-правовой объект – защиту персональных данных личности.

УДК 343.23

Е.А. Воропай

ОТДЕЛЬНЫЕ АСПЕКТЫ ОБЪЕКТА И ОБЪЕКТИВНОЙ СТОРОНЫ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ

Проблема борьбы с коррупцией стала в последние годы одной из наиболее актуальных: интерес к ней возрос как в обществе, так и на страницах научных изданий. В средствах массовой информации это явление справедливо рассматривается как серьезный барьер на пути развития здорового общества, как социальное зло, требующее вмешательства государства.

Как известно, санкция – это показатель характера и степени общественной опасности деяния, запрещенного уголовным законом. При ее установлении решающее значение имеет оценка значимости (социальной ценности) объекта преступления. По коррупционным преступлениям четко прослеживается специфика объекта преступного посягательства.

Значимость объекта коррупционных преступлений требует единой позиции в конструировании санкций за их совершение. Они должны быть достаточно строгими и отличаться лишь в зависимости от характера общественной опасности совершаемого деяния. В этой связи можно признать достаточно оправданной политику государства, направленную на усиление борьбы с коррупционными преступлениями. Однако и в данном случае должны быть разумные, сбалансированные подходы.

Объект коррупционных преступлений в его едином понимании в теории уголовного права не определен. Он определяется применительно к каждому преступлению, предусмотренному в различных разделах и главах УК.

Следует согласиться с мнением С.В. Максимова о том, что коррупционные преступления представляют собой предусмотренные УК «общественно опасные деяния, непосредственно посягающие на авторитет публичной службы, выражающиеся в незаконном получении государственными или муниципальными служащими каких-либо преимуществ (имущества, прав на него, услуг или льгот) либо в предоставлении последним таких преимуществ». При этом авторитет публичной власти, государственной службы и службы в органах местного самоуправления может выступать как основным, так и обязательным дополнительным непосредственным объектом преступного посягательства либо факультативным его объектом. А.Е. Воло-