ция о новых аналогичных преступлениях. Как правило, чем более жестокой является расправа над животным, тем большую известность получает ее исполнитель.

Отдельного внимания требуют общественно опасные деяния, ответственность за которые установлена в гл. 30 УК: изготовление и распространение порнографических материалов или предметов порнографического характера (ст. 343 УК), в том числе с изображением несовершеннолетнего (ст. 343[1] УК). Применительно к ним социальные сети следует рассматривать не только в контексте причин и условий, способствующих совершению данных преступлений, но и как средство их совершения в части, касающейся распространения порнографических материалов, поскольку такие материалы чаще всего представляют собой файлы в различных фото- и видеоформатах, для передачи которых социальные сети предоставляют очень широкие возможности. Подчеркивая актуальность данной проблемы, заметим, что по состоянию на 14 марта 2018 г. в социальной сети «ВКонтакте» по запросу «порнография» поисковой системой было обнаружено 19 467 соответствующих сообществ. Численность подписчиков наиболее популярного из них составляла более 850 тыс. человек. При этом у 185 групп в графе «регион регистрации» была прямо указана Республика Беларусь.

Отметим также, что в последние годы социальные сети могут не только выступать как средство передачи информации, но и использоваться для приема платежей благодаря разработке внутренних платежных систем при распространении как порнографических материалов, так и иных фотоматериалов и видеозаписей, примеры которых приводились выше. Так, в социальной сети «ВКонтакте» в июне 2018 г. появилась система VK Pay, доступная только гражданам Российской Федерации. Следовательно, ни одного факта совершения преступлений с ее использованием в нашей стране до настоящего времени зафиксировано не было. Однако, учитывая тенденцию активной адаптации преступности к условиям современного технического прогресса и стремительного изменения на этом фоне механизмов преступного поведения, можно обоснованно предположить, что по мере своего развития электронные средства платежа социальных сетей будут использоваться для совершения различных преступлений и в Республике Беларусь.

Таким образом, приведенные выше примеры свидетельствуют о том, что в современных условиях развития общества социальные сети активно включены в механизм индивидуального преступного поведения на различных его этапах – от мотивации и приготовления до размещения информации о совершенном деянии, влияя тем самым на состояние преступности в целом. Мониторинг социальных сетей, в частности определенных тематических сообществ и персональных страниц лиц, представляющих оперативный интерес, как со стороны компетентных государственных органов, так и со стороны общественности может способствовать не только выявлению уже совершенных преступлений, но и пресечению планируемых. Общие тенденции адаптации преступности к новым условиям технического прогресса позволяют выделить одно из перспективных направлений ее развития – использование внутренних платежных систем социальных сетей для получения доходов от преступной деятельности, а значит, профилактические меры в обозначенном процессе целесообразно начинать разрабатывать уже в настоящее время.

УДК 343.2.7

В.В. Вабищевич

ОТДЕЛЬНЫЕ АСПЕКТЫ ОПРЕДЕЛЕНИЯ СУБЪЕКТОВ ПОСЯГАТЕЛЬСТВ НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ

В современном мире наблюдается повсеместное использование информации, содержащей данные о конкретном лице, например, в оперативно-розыскной деятельности, в финансовой и налоговой отраслях, в сфере пенсионного, социального, медицинского страхования, в трудовых отношениях и других областях общественной жизни. Столь широкое использование персональных данных может создавать угрозу нарушений прав человека.

Эксперты отмечают, что в сфере информационной безопасности важной темой стали персональные данные, которые являются для разработчиков сервисов и приложений, владельцев различных агентств и, конечно, злоумышленников одним из ценных и желанных товаров в мире информационных технологий. Специалистами также обозначено, что не все пользователи осознают необходимость сохранности личной информации.

В Республике Беларусь специализированный нормативный правовой акт в сфере защиты и оборота персональных данных еще не принят, наше государство не присоединилось к Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Как следствие, в УК Республики Беларусь отсутствуют специальные составы преступлений, непосредственный объект которых – защита персональных данных. Для сравнения отметим, что уголовная ответственность за сам факт посягательств на персональные данные предусмотрена в странах Европейского союза, Канаде, Казахстане, Японии, Китае, США и других государствах.

Работа над проектом закона Республики Беларусь о защите персональных данных уже ведется. В ст. 20 проекта закона установлено, что «лица, виновные в нарушении требований настоящего Закона, несут ответственность, предусмотренную законодательными актами».

В КоАП внесены изменения в части ответственности за посягательства на персональные данные. Согласно новой редакции ст. 22.13 КоАП к административной ответственности привлекается лицо, которое допустило умышленное незаконное разглашение персональных данных, имея к ним доступ в связи с выполнением профессиональной или служебной деятельности, если в этих деяниях нет состава преступления.

Одним из следующих шагов должно стать формирование уголовно-правового состава, объектом защиты которого станут общественные отношения в сфере оборота персональных данных. С этой целью необходимо проработать вопрос о таком элементе состава преступления, как субъект совершения посягательств на персональные данные. К преступным посягатель-

ствам могут относиться действия, связанные с хищением персональных данных, их незаконным сбором, обезличиванием, хранением и т. д., непринятием мер по обеспечению сохранности персональных данных и их защите.

Под субъектом преступления понимается лицо, осуществляющее воздействие на объект уголовно-правовой охраны и способное нести за это ответственность. Субъект посягательств на персональные данные в определенной степени тождественен с субъектом посягательств на информационную безопасность, однако имеет определенные особенности.

В сфере информационной безопасности известный советский и российский ученый Е.П. Ищенко выделяет следующие группы преступников:

хакеры – лица, рассматривающие меры защиты информационных систем как личный вызов и взламывающие их с целью получения контроля за информацией независимо от ее ценности;

шпионы – лица, взламывающие защиту информационных систем для получения информации, которую можно использовать в целях политического влияния;

террористы – лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать и в целях политического влияния;

корпоративные налетчики – служащие компании, взламывающие компьютеры конкурентов для экономического влияния;

воры – лица, вторгающиеся в информационные системы для получения личной выгоды;

вандалы – лица, взламывающие системы с целью их разрушения;

нарушители правил пользования ЭВМ, совершающие противоправные действия из-за недостаточного знания техники и порядка пользования информационными ресурсами;

лица с психическими аномалиями, страдающие новым видом заболеваний – информационными болезнями или компьютерными фобиями.

Как видно из данной классификации, все виды субъектов связаны со взломом информационных систем, использованием компьютеров и иных автоматизированных технологий. Цели у преступников разные, однако всех их объединяет профессиональная возможность совершать данные преступления.

Взламывать информационные системы и похищать личную информацию граждан также могут субъекты посягательств на персональные данные. Однако только малая часть субъектов совершают такие деяния.

Общий возраст, с которого наступает уголовная ответственность за преступления против информационной безопасности, составляет шестнадцать лет, в то время как посягательства на персональные данные часто совершают лица в возрасте от четырнадцати до шестнадцати лет, а также малолетние. Например, недавно подростки украли жесткие диски с личными данными учеников и использовали их в личных целях.

Одним из видов посягательств на персональные данные является киберпреследование, которое отличается тем, что виктимизации подвергается одна и та же жертва, а преступление представляет собой цепочку инцидентов разной степени тяжести, которые стабилизируют постоянное и продолжительное влияние преступника на пострадавшую сторону. Нередко главным средством совершения такого преследования является использование персональных данных, позволяющих манипулировать личностью.

Особый вид субъектов посягательств на персональные данные – сотрудники коммерческих компаний, действующие по поручению своих руководителей. Часто незаконный сбор персональной информации не связан со взломом информационных систем, так как преступники используют ухищренные способы получения персональной информации, пользуясь халатностью самих потерпевших.

Специфической категорией субъектов, осуществляющих посягательства на персональные данные, являются представители государственных органов, иных организаций, осуществляющих сбор персональных данных либо имеющих доступ к этим данным. В Республике Беларусь существует более сотни различных баз персональных данных во всех сферах жизнедеятельности. С одной стороны, сотрудники имеют открытый доступ к таким базам для выполнения производственных заданий, а с другой стороны, могут использовать персональные данные в личных целях, не связанных со служебной деятельностью.

Таким образом, субъекты посягательств на персональные данные представлены достаточно широким кругом граждан разных сфер жизнедеятельности, разного возраста. Это профессиональные хакеры, сотрудники коммерческих организаций и государственных органов, и не только работающие, но и безработные, учащиеся и т. д. Классификация субъектов посягательств на персональные данные зависит от целей посягательства, например в рамках киберпреследования субъектом может быть бывший супруг либо сосед, коллега по работе. Указанное следует принимать во внимание при формировании специального уголовно-правового состава, направленного на криминализацию посягательств на персональные данные, при осуществлении предупредительной и профилактической деятельности правоохранительных органов.

УДК 343.352

В.М. Веремеенко

ВЛИЯНИЕ ОБМАНА И ЗАБЛУЖДЕНИЯ НА КВАЛИФИКАЦИЮ ВЗЯТОЧНИЧЕСТВА

Проблема взяточничества входит в число актуальных проблем современной политики государства. Основополагающим инструментом минимизации негативных последствий преступлений, составляющих взяточничество, является эффективное применение уголовного закона, отдельное звено которого – это правильная квалификация содеянного виновными лицами. Анализ судебной и следственной практики по делам данной категории свидетельствует о сложности этого процесса, много-