УДК 343.4

В. В. Вабищевич
исследователь, магистр права

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ПЕРСОНАЛЬНЫХ ДАННЫХ: ОТДЕЛЬНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ

Аннотация. В статье раскрывается научно-практическая стратегия уголовно-правовой охраны персональных данных, основанная на введении отдельных, усиливающих уголовную ответственность квалифицирующих признаков преступных посягательств на персональные данные, а также на необходимости системного принятия конкретных мер, направленных на предупреждение криминологических рисков преступных посягательств на персональные данные в целях обеспечения защиты конституционных прав и свобод человека и гражданина, а также информационной безопасности личности.

Ключевые слова: персональные данные; защита информации; совершенствование уголовного закона; информационная безопасность; посягательства на персональные данные.

Введение. Персональные данные стали самостоятельным объектом конституционной охраны в связи с принятием новой редакции Конституции Республики Беларусь, в соответствии со ст. 28 которой государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании.

В последние годы в Беларуси принимаются комплексные меры, направленные на создание условий для защиты персональных данных. Результативность работы заинтересованных лиц и государственных органов, научного сообщества и практиков, направленная на усиление правовой регламентации обработки персональных данных, критериев их определения, мер надлежащей защиты, в том числе введения ответственности за посягательства на них, не вызывает сомнений. Важное значение имеет введение в Уголовный кодекс Республики Беларусь (далее — УК) новых составов преступлений (ст. 203-1 и 203-2), непосредственным объектом охраны которых стали персональные данные.

Вместе с тем общественные отношения в сфере обработки персональных данных развиваются стремительными темпами. Необходимо констатировать значительное количество криминологических рисков преступных посягательств на персональные данные: всеобщая информатизация; прогрессивная государственная политика, направленная на построение «цифрового» государства; развитие искусственного интеллекта; трансграничность информационных систем; рост пользователей сети Интернет; низкая грамотность в правовой и информационной сферах; сложный процесс расследования уголовных дел; виктимность; вовлечение малолетних; корпоративная халатность при обработке персональных данных и др.

Согласно подп. 41.13 Концепции правовой политики Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 28 июня 2023 г. № 196, в сферах конституционного законодательства и законодательства о государственном управлении необходимо своевременно актуализировать законодательство и совершенствовать практику обработки персональных данных. В соответствии с ч. 2 п. 78 Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, множественные угрозы и риски незаконного и необоснованного вмешательства в частную жизнь граждан, похищение персональных данных, компрометация реквизитов доступа и избыточное профилирование сужают личное пространство человека и нарушают его приватность.

Непосредственные исследования по вопросу уголовно-правовой охраны персональных данных в отечественной доктрине фактически отсутствуют, поскольку наблюдается концентрация внимания на детальном изучении проблем самого института персональных данных как объекта конституционного и гражданского права. Наиболее значимые исследования по вопросам ответственности за незаконные действия с персональными данными и информацией о частной жизни (либо усиления защиты персональных данных) в белорусской юридической науке нашли отражение в публикациях отдельных авторов (М. С. Абламейко, М. А. Дубко, Д. Г. Полещук, Н. А. Саванович, О. О. Топорикова, А. А. Шугай и др.).

В целях дальнейшего совершенствования уголовно-правовой охраны персональных данных детального исследования требуют следующие проблемы:

– сокращен круг деяний, которые могут расцениваться в качестве преступных. Уголовно-противоправными являются только незаконные сбор, предоставление, распространение и несоблюдение мер обеспечения защиты персональных данных;

– отсутствуют критерии разграничения персональных данных и информации о частной жизни, в том числе их уголовно-правовой охраны;

– не проработана самостоятельная криминализация посягательств на персональные данные, сопряженных с совершением преступлений против компьютерной безопасности;

– квалифицирующие признаки не учитывают в полной мере специфику элементов составов преступлений, относящихся к предмету, объекту преступления, месту распространения персональных данных, субъекту, субъективной стороне и др.

В настоящей статье представлен авторский взгляд о направлениях дальнейшего совершенствования уголовно-правовой охраны персональных данных, о выработке научно-практической стратегии уголовно-правовой охраны персональных данных, учитывающей международный опыт, достижения современной юридической науки и развитие национального законодательства.

Основная часть. Уголовно-правовая охрана персональных данных непосредственно взаимосвязана с обеспечением национальной безопасности через призму информационной безопасности личности и государства. Защищенность и сохранность персональных данных являются одной из важных задач информационной безопасности государства, которая выступает неотъемлемой частью национальной безопасности, а новые формы информационных войн («гибридные» и «цветные» революции, вмешательства во внутренние дела государства и т. д.) предполагают работу с огромным массивом ограниченных в доступе персональных данных, которые собираются как самостоятельно, так и с помощью лиц, передающих эти данные из личной и иной заинтересованности.

Следует согласиться с О. С. Макаровым, который отмечает, что «одним из важнейших параметров национальной безопасности государств и актуальнейшим направлением ее государственного обеспечения является информационная безопасность» [1, с. 3]. Так, например, прокуратура города Минска направила в суд уголовное дело в отношении 32-летнего мужчины, которому инкриминированы незаконный сбор и распространение информации о частной жизни и персональных данных, публичные призывы к действиям, направленным на причинение вреда национальной безопасности Республики Беларусь [3].

Р. Н. Ключко, О. И. Семыкина отмечают, что «интенсивная цифровая трансформация меняет подход к пониманию прежде всего информационной безопасности. Сегодня информационная безопасность, во-первых, является неотъемлемым элементом информационных отношений, во-вторых, сопряжена с обеспечением информационного суверенитета и, в-третьих, выступает дополнительным объектом всех преступлений против прав, свобод и законных интересов личности, общества и государства, совершаемых посредством цифрового воздействия» [2, с. 34].

При умышленной незаконной трансграничной передаче персональных данных в целях причинения вреда национальной безопасности под негативное воздействие могут подпадать два самостоятельных (конкурирующих) объекта: конституционные права и свободы человека и гражданина и интересы государства. При этом уголовно-правовая охрана конституционных прав и свобод человека и гражданина должна являться приоритетной, но только при отсутствии признаков более тяжких преступлений против государства.

Существующие теоретические и правовые подходы к определению термина «информационная безопасность личности» носят узкий характер, включающий в себя только влияние негативной информации на личность. Предлагается на законодательном уровне дать определение термину «информационная безопасность личности — состояние, при котором отсутствует риск, связанный с причинением информацией, в том числе путем совершения незаконных действий с персональными данными, вреда физическому, психическому, нравственному, духовному и соци-

альному развитию личности, а также созданы условия для доступа к способствующей ее надлежащему развитию информации и меры по защите ее персональных данных». Данное предложение позволит рассматривать информационную безопасность личности в широком смысле, включая защиту персональных данных, а также может стать предпосылкой для концептуальной проработки вопроса о формировании в уголовном праве нового родового объекта — информационной безопасности личности.

Международно-правовое регулирование защиты персональных данных, зарубежный опыт уголовно-правовой охраны свидетельствуют о необходимости установления конкретной уголовной ответственности за посягательства на персональные данные, учитывая разграничение между уголовно-правовой охраной персональных данных и информации о частной жизни; широкий набор квалифицирующих признаков, влияющих на степень тяжести совершенных преступлений и условия привлечения виновных лиц к уголовной ответственности; повышенную уголовную ответственность за посягательства на специальные персональные данные [4; 5].

Немаловажным является установление соотношения понятий «персональные данные» и «информация о частной жизни», а также иных схожих понятий, что позволит проанализировать и дать оценку подходу об исключении из УК ст. 179, а также в определенном смешении в ст. 203-1 понятий «персональные данные» и «информация о частной жизни».

Понятие «персональные данные» не является тождественным понятию «информация о частной жизни» либо его составной частью. Отсутствуют критерии разграничения информации о частной жизни от персональных данных, либо установления тождественности и идентичности данных понятий, либо определения их соотношения как общего и частного. В законодательстве Республики Беларусь отсутствует определение термина «информация о частной жизни».

В целях разграничения уголовно-правовой охраны информации о частной жизни и персональных данных с учетом объекта, объективной стороны и предмета преступных посягательств предлагается самостоятельная регламентация уголовно-правовой охраны информации о частной жизни, а также дополнение УК

термином «информация о частной жизни». При этом под информацией о частной жизни следует понимать «сведения, раскрывающие личную и семейную тайну человека, его поведение и жизнедеятельность, включая домашнюю, физическую и духовную сферы, не связанные с профессиональной, служебной или предпринимательской деятельностью». В качестве критериев разграничения можно выделить следующие:

- содержательность (вид сведений — публичный (фамилия, имя и т. п.), частный (духовная сфера, личные связи));
- среда формирования (взаимосвязь с неопределенным незнакомым либо определенным знакомым кругом лиц);
- доступность (сведения находятся в открытом доступе, распространяются самим субъектом либо необходимо предпринять определенные действия для сбора соответствующей информации);
- объективность (информация действительно в определенном социуме воспринимается как частная (личная));
- ценность (обладание данной информацией третьим лицом позволяет получить определенные выгоды).

Кроме того, совершение умышленной незаконной обработки персональных данных в отношении специальных персональных данных, которые имеют наибольшую ценность для человека, должно рассматриваться как отягчающий уголовную ответственность виновного лица признак.

Принятие Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее — Закон № 99-З) обусловило надлежащее урегулирование общественных отношений в сфере обработки персональных данных, во многом оказав влияние на введение в УК ст. 203-1, 203-2. Однако, на наш взгляд, ст. 203-1, 203-2 УК в значительной степени сужают круг потенциальных нарушений, которые могут привести к существенному вреду правам, свободам и законным интересам граждан.

Под обработкой персональных данных в соответствии с Законом № 99-З понимается любое действие или совокупность действий, совершаемых с персональными данными, включая сбор, систематизацию, хранение, изменение, использование,

обезличивание, блокирование, распространение, предоставление, удаление персональных данных. Предлагается установить уголовную ответственность за умышленную незаконную обработку персональных данных другого лица, повлекшую причинение существенного вреда правам, свободам и законным интересам гражданина, что позволит криминализировать любое незаконное действие (бездействие) с персональными данными, повлекшее достаточные для уголовной ответственности последствия, а не только сбор, предоставление и распространение персональных данных.

Необходимо также в ст. 203-2 УК расширить круг действий, направленных на ознакомление с персональными данными неопределенного круга лиц и повлекших причинение тяжких последствий, а не только несоблюдение мер обеспечения защиты персональных данных, необходимость выполнения которых в настоящее время предусмотрена только к определенной сфере правового регулирования (в рамках Закона № 99-З).

Становление персональных данных как самостоятельного юридического института напрямую взаимосвязано с развитием компьютерных технологий, сети Интернет, СМИ как в печатных, так и в электронных изданиях, переходом к электронному взаимодействию. Кроме того, в настоящее время сложно представить преступные посягательства на персональные данные без использования компьютерных технологий либо не нарушающих компьютерную безопасность, а распространение персональных данных приносит наиболее существенный вред правам и свободам человека и гражданина, когда совершается публично.

Некоторые ученые отмечают, что законодатель не выделил «использование глобальной компьютерной сети Интернет» в качестве самостоятельного квалифицирующего признака, а использовал именно термин «распространение». Предложенный подход позволяет сохранить «технологическую нейтральность» уголовного закона [6, с. 731].

При этом именно использование сети Интернет свойственно при посягательствах на персональные данные. Например, прокуратура г. Гродно при мониторинге информации в сети Интернет

установила, что участники деструктивных Telegram-каналов распространили информацию о частной жизни, персональные данные заместителя начальника отдела прокуратуры [7].

С целью усиления уголовной ответственности для лица, придавшего публичную огласку персональным данным, бесконтрольность распространения которых в СМИ и сети Интернет делает фактически невозможным их удаление в целях восстановления нарушенных прав потерпевшего, предлагается в отношении умышленного незаконного распространения персональных данных, повлекшего причинение существенного вреда правам, свободам и законным интересам гражданина, введение квалифицирующего признака — «в средствах массовой информации, либо в информации, размещенной в глобальной компьютерной сети Интернет, либо в иной информационной сети».

Посягательства на персональные данные путем совершения преступлений против компьютерной безопасности должны рассматриваться в качестве киберпреступлений и подлежать самостоятельной криминализации путем введения дополнительного квалифицирующего признака — «совершение умышленной незаконной обработки персональных данных путем несанкционированного доступа к компьютерной информации либо неправомерным ее завладением, уничтожением, блокированием, модификацией».

Генеральный прокурор Республики Беларусь А. И. Швед сообщил, что «абсолютное большинство составляют хищения путем использования компьютерной техники. Все активнее информационные технологии используются при совершении мошенничеств, вымогательств, заведомо ложных сообщений об опасности, разглашении персональных и других охраняемых данных, преступлений экстремисткой направленности» [8].

В гл. 31 УК персональные данные не рассматриваются как предмет, опосредующий отягчение уголовной ответственности в случае, например, неправомерного завладения компьютерной информацией (ст. 352 УК), когда в качестве такой информации выступают персональные данные.

Указанная неполноценная защищенность персональных данных противоречит практике совершения посягательств на персональные данные посредством совершения преступлений против компьютерной безопасности. Названная проблематика, по

нашему мнению, связана с тем, что посягательства на персональные данные с использованием компьютерных технологий в первую очередь рассматриваются как преступления против компьютерной безопасности, а не конституционных прав и свобод граждан, то есть в качестве киберпреступлений, предметом посягательства которых (исключая ст. 212, 216 УК) являются компьютерная техника и компьютерная информация, машинные носители и т. д.

Целесообразности расширения перечня киберпреступлений за счет включения в их состав посягательств на персональные данные путем совершения преступлений против компьютерной безопасности придерживаются многие специалисты, отмечая, что расширение перечня кибер- и интернет-преступлений включает объединение их по предмету и средству совершения преступления, а именно (в качестве примера): деяния, направленные на незаконные действия на компьютерную информацию, которая содержит персональные данные [9, с. 183]; кража персональной информации является киберпреступлением, если она происходит с использованием компьютерных технологий и сети Интернет [10].

Предложение о введении соответствующего квалифицирующего признака (путем совершения определенных посягательств на компьютерную безопасность) в ст. 203-1 УК связано с нецелесообразностью, по нашему мнению, указывать на персональные данные как на квалифицирующий признак при совершении преступлений против компьютерной безопасности, когда дополнительным предметом посягательств выступают персональные данные (например, хищение компьютерной информации, когда в качестве такой информации выступают персональные данные полностью либо в части). Дополняя соответствующие статьи главы 31 УК персональными данными, возникнет вопрос о посягательствах на иные объекты и предметы уголовно-правовой охраны, например коммерческую или банковскую тайну, государственные секреты и т. д., которые, следуя принципам последовательности, также должны содержаться в статьях главы 31 УК, что не является оправданным. Кроме того, преступным является не только сам факт, например, незаконного

сбора персональных данных, но и причинение существенного вреда правам и свободам граждан, их законным интересам.

Мотив и цель преступления, как психологические признаки совершаемого деяния, указывают на волевую направленность деяния и, по нашему мнению, имеют особое значение, поскольку сами по себе посягательства на персональные данные зачастую не являются самоцелью, а нарушение законодательства о персональных данных не всегда автоматически причиняет существенный вред либо тяжкие последствия общественным отношениям. Кроме того, посягая на персональные данные, виновник, как правило, преследует достижение иных целей, в том числе совершение более тяжких преступлений.

Совершение одних преступлений в целях совершения других является по своей сути наиболее тяжким преступлением. Персональные данные зачастую выступают средством совершения других преступлений. Криминализации может подлежать незаконная обработка персональных данных, совершенная в целях совершения следующих преступлений: ст. 130 УК (разжигание расовой, национальной, религиозной либо иной социальной вражды или розни), ст. 145 УК (доведение до самоубийства), ст. 185 УК (принуждение), ст. 208 УК (вымогательство), ст. 254 УК (коммерческий шпионаж), ст. 288 УК (принуждение лица к участию в преступной деятельности), ст. 365 УК (вмешательство в деятельность сотрудника органов внутренних дел), ст. 384 УК (принуждение к выполнению обязательств), ст. 389 УК (угроза в отношении судьи или народного заседателя), ст. 404 УК (принуждение свидетеля, потерпевшего или эксперта к отказу от дачи показаний или заключения либо к даче ложных показаний или заключения), ст. 408 УК (умышленное разглашение сведений о мерах безопасности, применяемых в отношении защищаемого лица), ст. 427 УК (служебный подлог). Незаконная обработка персональных данных может рассматриваться в качестве способов совершения вышеназванных преступлений, поскольку в них предполагается разглашение сведений либо иная манипуляция с ними, которые должны привести к достижению преступного результата.

Кроме того, особое внимание необходимо уделить усилению уголовной ответственности для лиц, совершающих посягательства на персональные данные, с использованием своих служебных (профессиональных) полномочий.

Заключение. Вышеизложенные направления совершенствования уголовно-правовой охраны сформированы с учетом комплекса криминологических рисков преступных посягательств на персональные данные, а также в своей совокупности предопределяют необходимость в стратегическом подходе: защита конституционных прав и свобод граждан уголовно-правовыми средствами, основанная на отграничении персональных данных от информации о частной жизни; дифференциация оснований и условий уголовной ответственности за посягательства на персональные данные; установление взаимосвязи уголовно-правовой охраны персональных данных и обеспечения информационной безопасности личности как элемента информационной и национальной безопасности.

Стратегия включает в себя также и принятие системных мер по предупреждению преступных посягательств на персональные данные. При этом меры предупреждения должны быть комплексными, направленными на все категории населения. Система мер должна учитывать все уровни и возможные направления деятельности, включая правовые (реализация предложенной комплексной научно-практической стратегии уголовно-правовой охраны персональных данных, а также совершенствование гражданского, административного, трудового законодательства), организационные (выстраивание взаимодействия между государственными органами и гражданским обществом, создание некоммерческой организации по защите прав субъектов персональных данных, включение вопросов защиты персональных данных в государственную программу по борьбе с преступностью, определение субъектом профилактики посягательств на персональные данные НЦЗПД), технические (обеспечение национального «цифрового» (технологического) суверенитета, разработка стандартов в сфере защиты персональных данных), образовательные (внедрение в образовательные программы (на всех ступенях) курсов, уроков, лекций и семинаров,

посвященных информационной безопасности и защите персональных данных, подготовка сотрудников правоохранительных органов), информационно-культурные (повышение правовой и информационной культуры, социальная реклама, работа со всеми категориями населения, учреждение дня по информационной безопасности личности и др.), криминалистические (совершенствование методов и инструментов расследования преступлений в сфере информационных технологий и компьютерной безопасности и др.) и др. При этом в эту работу должны быть вовлечены как профессиональные участники (НЦЗПД, правоохранители и т. д.), так и общественные, социальные и образовательные структуры, гражданское общество, СМИ.

Список использованных источников

1. Макаров, О. С. Правовое обеспечение информационной безопасности на примере защиты государственных секретов государств — участников Содружества Независимых Государств : автореф. дис. … д-ра юрид. наук: 12.00.13 / О. С. Макаров. — М., 2013. — 52 с.
2. Семыкина, О. И. «Цифровой» признак совершения преступлений как вектор криминализации (компаративный обзор подходов государств — участников СНГ) / О. И. Семыкина, Р. Н. Ключко // Журн. зарубеж. законодательства и сравн. правоведения. — 2020. — № 6. — С. 34–52.
3. В суд направлено уголовное дело в отношении разработчика приложения деструктивной направленности [Электронный ресурс] // Генеральная прокуратура Республики Беларусь. — Режим доступа: https://prokuratura.gov.by/ru/media/novosti/nadzor-za-resheniyami-po-ugolovnym-i-grazhdanskim-delam/v-sud-napravleno-ugo3/. — Дата доступа: 19.09.2023.
4. Вабищевич, В. В. Зарубежный опыт уголовно-правовой охраны персональных данных / В. В. Вабищевич // Журн. Белорус. гос. ун-та. Право. — 2019. — № 1. — С. 72–80.
5. Вабищевич, В. В. Правовая охрана персональных данных в контексте их международно-правовой защиты / В. В. Вабищевич // Вестн. Белорус. гос. экон. ун-та. — 2021. — № 3 — С. 107–118.
6. Полещук, Д. Г. Уголовно-правовая охрана общественных отношений в сфере обеспечения информационной безопасности: проблема понимания и направления совершенствования уголовного закона / Д. Г. Полещук // Право в современном белорусском обществе : сб. науч.

тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, Ин-т правовых исследований. — Минск, 2020. — Вып. 15. — С. 726–736.

7. Прокуратура Гродно: возбуждены уголовные дела за незаконное распространение информации о частной жизни и персональных данных [Электронный ресурс] // Генер. прокуратура Респ. Беларусь. — Режим доступа: https://prokuratura.gov.by/ru/media/novosti/nadzor-za-reshe-niyami-po-ugolovnym-i-grazhdanskim-delam/prokuratura-grodno-vozbuzh-deny-ugolovnye-dela-za-nezakonnoe-rasprostranenie-informatsii-o-chast-noy-zh/. — Дата доступа: 20.09.2023.

8. Безопасность в сфере использования информационно-коммуникационных технологий: в Москве состоялось заседание Объединенной коллегии генеральных прокуратур Беларуси и России [Электронный ресурс] // Генеральная прокуратура Респ. Беларусь. — Режим доступа: https: https://prokuratura.gov.by/ru/activity/media/detail/mezhdunarodnoe-sotrudnichestvo/bezopasnost-v-sfere-ispolzovaniya-informatsionno-kom-munikatsionnykh-tekhnologiy-v-moskve-sostoyalos-/. — Дата доступа: 19.09.2023.

9. Зигмунт, О. А. Кибер- и интернет-преступность в Германии и России: возможности сравнительного исследования / О. А. Зигмунт, А. В. Петровский // Юрид. наука и правоохран. практика. — 2015. — № 4. — С. 180–188.

10. Лимож, Н. Киберпреступления: особенности совершения и предупреждения [Электронный ресурс] / Н. Лимож, М. Косович // ООО «Профессиональные правовые системы». — 2017–2020. — Режим доступа: http://bii.by/tx.dll?d=301093&a=10. — Дата доступа: 26.09.2023.

02.11.2023

V. V. Vabishchevich
researcher, Master of Law

CRIMINAL LEGAL PROTECTION OF PERSONAL DATA: SELECTED AREAS OF IMPROVEMENT

Annotation. The article reveals the scientific and practical strategy of criminal and legal protection of personal data, based on the introduction of separate qualifying elements of criminal encroachments on personal data that strengthen criminal liability, as well as the need for systematic adoption of specific measures aimed at preventing criminological risks of criminal encroachments on personal data in order to ensure the protection of constitutional rights and freedoms of man and citizen, as well as personal information security.

Key words: personal data; information protection; improvement of criminal law; information security; encroachments on personal data.