

к анализу и оценке количественных и качественных показателей административной деликтности.

Список использованных источников:

1. Дерюга, А.Н. Задачи административной деликтологии на современном этапе / А.Н.Дерюга // Государство и право. – 2010. – № 2. – С. 5–12.
2. Мышляев, Н.П. Теоретические и прикладные основы административной деликтологии: автореф. ... д-ра юрид. наук: 12.00.14 / Н.П.Мышляев. – М., 2004. – 46 с.
3. Никулин, М.И. Проблемы науки административной деликтологии: автореф. дис. ... д-ра юрид. наук: 12.00.14 / М.И.Никулин. – М., 2005. – 50 с.
4. Гензюк, Э.Е. Административная деликтология: автореф. ... д-ра юрид. наук: 12.00.14 / Э.Е.Гензюк. – М., 2001.
5. Дерюга, А.Н. Соотношение административной деликтологии и статистики / А.Н.Дерюга // Вестн. Московского ун-та МВД России. – 2010. – № 1. – С. 90–92.

Лосев Владимир Владимирович

**НЕЗАКОННЫЕ СБЫТ И ПРИОБРЕТЕНИЕ БАЗ ПЕРСОНАЛЬНЫХ
ДАННЫХ: ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ
ПРЕДПРИЯТИЙ**

Профессор кафедры государственно-правовых дисциплин, факультет права,
Белорусский государственный экономический университет, кандидат
юридических наук, доцент, Losev.Lv@yandex.ru

Аннотация. В статье проведено комплексное исследование ответственности должностных лиц за незаконные сбыт и приобретение баз персональных данных – уголовной, административной, дисциплинарной и гражданско-правовой ответственности. Охарактеризованы действия, образующие незаконную обработку персональных данных. Выделены проблемные вопросы их квалификации. Сформулированы предложения о правилах юридической оценки нарушений должностными лицами законодательства о защите персональных данных и прав субъектов персональных данных.

Ключевые слова: персональные данные, базы данных, сбыт, приобретение, ответственность, должностные лица, квалификация.

В 2021 г. был принят Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», а также внесены изменения и дополнения в части установления ответственности за незаконные действия с персональными данными в Уголовный кодекс Республики Беларусь (далее – УК), Кодекс Республики Беларусь об административных правонарушениях (далее – КоАП) и в Трудовой кодекс Республики Беларусь (далее – ТК), а также в Декрет

Президента Республики Беларусь от 15 декабря 2014 г. № 5 «Об усилении требований к руководящим кадрам и работникам организаций».

В хозяйственной деятельности давно уже получила широкое распространение практика незаконного сбора баз персональных данных для целей рекламной рассылки, привлечения покупателей и клиентов. Утечки баз персональных данных и, как следствие, спам-рассылка, звонки с незнакомых номеров, неправомерный доступ к банковским счетам граждан, «телефонное мошенничество» стали уже повседневностью.

Наиболее громкими примерами служат подобные инциденты, выявленные в этом году Национальным центром защиты персональных данных: в июле 2022 г. – утечка персональных данных 635 тыс. участников программы лояльности торговой сети «Соседи»; в октябре 2022 г. – утечка персональных данных 148 тыс. клиентов ЧТУП «ЗападХимТорг» (бренд «Остров чистоты и вкуса»), а также утечка данных пользователей сервиса доставки еды «Just-eat» (ООО «ФУД КЛАБ»).

В связи с этим приобрели особую актуальность вопросы юридической оценки нарушений законодательства о защите персональных данных, прежде всего незаконных сбыта и приобретения персональных данных, совершенных должностными лицами с использованием своих служебных полномочий.

Проблематика ответственности за незаконные действия в отношении информации о частной жизни и персональных данных стала исследоваться в Беларуси сравнительно недавно. В последние годы ей уделили внимание, в частности, В.В. Вабищевич [1; 2], Д.Г. Полещук [3; 4; 5; 6; 7], который в 2020 г. защитил кандидатскую диссертацию на тему «Уголовно-правовая охрана информационной безопасности (на примере отдельных аспектов охраны кибербезопасности и защиты информации ограниченного распространения)» [7], А.А. Пухов [8], Н.А. Саванович [9]. Ученые исследовали планируемые и состоявшиеся изменения в законодательстве, формулировали предложения по совершенствованию норм УК, рассматривали отдельные вопросы ответственности.

Сейчас требуется комплексный подход к определению правил юридической оценки незаконных действий должностных лиц с персональными данными.

Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон о защите персональных данных) вступил в силу 15 ноября 2021 г. Его действие распространяется на все государственные органы, юридические лица (всех форм собственности), иные организации (далее – организации), на всех физических лиц, в том числе индивидуальных предпринимателей, которые самостоятельно или совместно с иными названными лицами организуют и (или) осуществляют любые действия с персональными данными, то есть их обработку, и тем самым являются «операторами».

Обработку персональных данных образуют любое действие или совокупность действий, совершаемые с персональными данными, включая

сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных (ст. 1 Закона о защите персональных данных).

Обязаны соблюдать требования Закона о защите персональных данных и «уполномоченные лица» – это государственные органы, юридические лица Республики Беларусь, иные организации, физические лица, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах (далее, говоря об операторах, подразумеваем и уполномоченных лиц, которые тоже осуществляют обработку персональных данных).

В соответствии с п. 1 ст. 16 Закона о защите персональных данных оператор наряду с иным обязан обеспечивать защиту персональных данных в процессе их обработки. Пункт 1 ст. 17 этого Закона обязывает оператора принимать правовые, организационные и технические меры по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обработку персональных данных и их защиту организуют и осуществляют должностные лица операторов, а именно руководители организаций, структурных подразделений, лица, назначенные ответственными за осуществление внутреннего контроля за обработкой персональных данных, а также другие работники, непосредственно осуществляющие такую обработку в процессе трудовой (служебной) деятельности.

Защиту персональных данных наряду с иными правовыми, организационными и техническими мерами обеспечивает установление ответственности:

уголовная ответственность за незаконные действия в отношении информации о частной жизни и персональных данных (ст. 203-1 УК) и несоблюдение мер обеспечения защиты персональных данных (ст. 203-2 УК);

административная ответственность за нарушение законодательства о защите персональных данных (ст. 23.7 КоАП);

дисциплинарная ответственность: нарушение работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных является основанием прекращения трудового договора, признаваемым дискредитирующим обстоятельством увольнения (п. 10 ст. 47 ТК, пп. 6.14-1 п. 6 Декрета Президента Республики Беларусь от 15 декабря 2014 г. № 5 «Об усилении требований к руководящим кадрам и работникам организаций»);

гражданско-правовая ответственность: подлежит возмещению моральный вред, причиненный субъекту персональных данных, независимо от возмещения имущественного вреда и понесенных субъектом убытков (п. 2 ст. 19 Закона о защите персональных данных).

Незаконными признаются действия с персональными данными, совершенные в нарушение требований Закона о защите персональных данных, т.е. без согласия субъекта персональных данных и при отсутствии иных правовых оснований обработки персональных данных, предусмотренных названным Законом (ст. 6 и 8, когда обработка совершается без согласия субъекта) и иными законодательными актами.

Под незаконным сбытом понимаются незаконные предоставление или распространение персональных данных:

предоставление – действия, направленные на ознакомление с персональными данными определенных лица или круга лиц;

распространение – действия, направленные на ознакомление с персональными данными неопределенного круга лиц.

Очевидно, что незаконное распространение персональных данных – это более опасное деяние, чем их предоставление.

Незаконное приобретение персональных данных охватывается понятием «сбор», т.е. получение персональных данных любым незаконным способом.

В ст. 203-1 УК предусмотрена уголовная ответственность за умышленные незаконные действия в отношении информации о частной жизни и персональных данных без согласия лица, если это повлекло причинение существенного вреда его правам, свободам и законным интересам: в ч. 1 – за сбор или предоставление такой информации; в ч. 2 – за ее распространение; в ч. 3 – за сбор, предоставление или распространение такой информации лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга.

Совершение должностным лицом незаконных действий в отношении информации о частной жизни и персональных данных посягает не только на конституционные права и свободы человека и гражданина, но и на интересы службы. В связи с этим возникает вопрос: охватываются ли совершенные должностным лицом с использованием своих служебных полномочий незаконные сбыт (предоставление, распространение), а равно приобретение (сбор) персональных данных только ст. 203-1 УК либо же требуется дополнительная квалификация как преступления против интересов службы?

Отметим, что ни в одной части ст. 203-1 УК не называется такой специальный субъект преступления, как «должностное лицо». И даже не подразумевается, поскольку не упоминается и признак «использование служебных полномочий».

В ч. 1 примечаний к гл. 35 «Преступления против интересов службы» УК сказано: «должностное лицо, которое использовало свои властные или иные служебные полномочия для совершения преступления, не названного в настоящей главе, несет ответственность по совокупности преступлений. При этом совершение такого преступления признается существенным вредом, предусмотренным статьями настоящей главы. Правило о совокупности преступлений не применяется, если совершение должностным лицом преступления предусмотрено в качестве признака иного преступления».

В связи с этим содеянное в названном случае, по нашему мнению, следует квалифицировать по совокупности преступлений, поскольку должностное лицо, используя свои служебные полномочия, совершает преступление, предусмотренное в гл. 23 «Преступления против конституционных прав и свобод человека и гражданина» УК, при этом ст. 203-1 УК не указывает (ни прямо, ни косвенно) должностное лицо в качестве специального субъекта незаконных действий в отношении информации о частной жизни и персональных данных. В таком случае налицо идеальная совокупность преступлений, а не конкуренция норм.

Поэтому деяние должностного лица наряду с соответствующей частью ст. 203-1 УК следует дополнительно квалифицировать как превышение служебных полномочий, повлекшее причинение существенного вреда правам и законным интересам граждан, по соответствующей части ст. 426 УК.

В п. 20 постановления Пленума Верховного Суда Республики Беларусь от 16 декабря 2004 г. № 12 «О судебной практике по делам о преступлениях против интересов службы (ст.ст. 424–428 УК)» (в редакции постановления Пленума Верховного Суда Республики Беларусь от 30 сентября 2021 г. № 7, далее – постановление № 12) сказано, что существенный вред может выражаться в том числе в нарушении конституционных прав и свобод граждан. Право гражданина на защиту от незаконного вмешательства в его частную жизнь в соответствии со ст. 28 Конституции Республики Беларусь является конституционным правом, при этом государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании.

Содеянное необходимо квалифицировать именно как превышение служебных полномочий, а не злоупотребление ими (ст. 424 УК), поскольку совершение должностным лицом иного умышленного преступления с использованием своих служебных полномочий, в том числе незаконных действий в отношении информации о частной жизни и персональных данных, очевидно является «действием, которое никто ни при каких обстоятельствах не вправе совершать», о чем как о признаке превышения власти или служебных полномочий прямо говорится в п. 14 постановления № 12.

Следует обратить внимание на то, что в соответствии с п. 19 ч. 1 ст. 33 УК незаконные действия в отношении информации о частной жизни и персональных данных, предусмотренные ч. 1 ст. 203-1 УК, а именно незаконные сбор и предоставление такой информации, влекут уголовную ответственность лишь при наличии выраженного в установленном уголовно-процессуальным законом порядке требования лица, пострадавшего от преступления, любого из его совершеннолетних близких родственников или членов семьи в случаях, предусмотренных уголовно-процессуальным законом, или его законного представителя либо представителя юридического лица привлечь виновного к уголовной ответственности. Ответственность же за преступления, предусмотренные ч. 2 и 3 ст. 203-1 УК, наступает независимо от требования пострадавшего.

Тем самым при отсутствии подобного требования пострадавшего совершенные должностным лицом при явном выходе за пределы прав и полномочий, предоставленных ему по службе, умышленные незаконные сбор или предоставление информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина, должны влечь ответственность только по соответствующей части ст. 426 УК (превышение власти или служебных полномочий).

При отсутствии существенного вреда правам, свободам и законным интересам гражданина умышленные незаконные сбыт и приобретение персональных данных образуют административное правонарушение, предусмотренное ст. 23.7 КоАП. Согласно ч. 2 этой статьи размер штрафа увеличивается до 100 базовых величин, если сбыт (предоставление) или приобретение (сбор) были совершены лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью (т.е. в том числе должностным лицом), и до 200 базовых величин, если лицом было совершено умышленное незаконное распространение персональных данных. Ответственность за административное правонарушение, предусмотренное ст. 23.7 КоАП, наступает независимо от требования потерпевшего или его законного представителя.

Увольнение должностного лица за такие незаконные действия с персональными данными по п. 10 ст. 47 ТК, пп. 6.14-1 п. 6 Декрета Президента Республики Беларусь от 15 декабря 2014 г. № 5 «Об усилении требований к руководящим кадрам и работникам организаций» не препятствует его привлечению к административной или уголовной ответственности.

Сформулированное автором мнение о квалификации подобных действий должностных лиц направлено на привлечение внимания к данной проблематике и активизацию дискуссии в этом направлении.

Список использованных источников

1. Вабищевич, В. Посягательства на персональные данные: направления криминализации / В. Вабищевич // Юстиция Беларуси. – 2020. – № 12. – С. 68–73.
2. Вабищевич, В. Уголовно-правовая охрана персональных данных в контексте обеспечения информационной безопасности / В. Вабищевич // Юстиция Беларуси. – 2020. – № 4. – С. 74–77.
3. Полещук, Д. Некоторые аспекты уголовно-правовой охраны информационной безопасности на примере защиты информации о частной жизни и персональных данных / Д. Полещук // Юстиция Беларуси. – 2020. – № 1. – С. 25–30.
4. Полещук, Д. Ответственность за незаконные действия с персональными данными: текущее состояние и перспективы / Д. Полещук // Законность и правопорядок. – 2020. – № 4. – С. 44–49.
5. Полещук, Д.Г. Уголовная ответственность за незаконные действия с персональными данными: новое в законодательстве и правоприменении [Электронный ресурс] : / Д. Г. Полещук // КонсультантПлюс Беларусь / ООО «ЮрСпектр», Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2022.

6. Полещук, Д.Г. Уголовно-правовая охрана информационной безопасности: актуальные проблемы теории и практики / Д. Г. Полещук; под науч. ред. Д. В. Шаблинской ; Нац. центр законодательства и правовых исследований Респ. Беларусь. – Минск : Колорград, 2022. – 239 с.

7. Полещук, Д.Г. Уголовно-правовая охрана информационной безопасности (на примере отдельных аспектов охраны кибербезопасности и защиты информации ограниченного распространения) : автореф. дис. ... канд. юрид. наук : 12.00.08 / Д. Г. Полещук. – Минск, 2020. – 32 с.

8. Пухов, А. Уголовно-правовая защита неприкосновенности частной жизни и персональных данных в свете изменений уголовного закона / А. Пухов // Право.by. – 2021. – № 4. – С. 85–92.

9. Саванович, Н.А. Уголовная ответственность за незаконные действия с персональными данными [Электронный ресурс] : / Н. А. Саванович. Режим доступа: <https://pravo.by/novosti/obyavleniya/2021/june/65306/>. – Дата доступа: 12.10.2022.

Минько Наталья Сергеевна

КОНСТИТУЦИОННОЕ ПОНИМАНИЕ ИНТЕГРАЦИОННОГО РАЗВИТИЯ (СТРОИТЕЛЬСТВА) БЕЛАРУСИ НА ЕВРАЗИЙСКОМ ПРОСТРАНСТВЕ: РЕТРОСПЕКТИВНЫЙ АНАЛИЗ

руководитель Центра государственного строительства и права ГНУ «Институт
экономики НАН Беларуси», кандидат юридических наук, доцент,
natallia.minko@gmail.com

Аннотация. В статье раскрываются основные этапы интеграционного развития (строительства) на территории белорусского государства, анализируются принятые акты конституционного значения. Вносятся ряд предложений, связанных с современными тенденциями развития Беларуси в составе интеграционных образований.

Ключевые слова: интеграционный конституционализм, интеграционное развитие (строительство), конституционные акты, акты конституционного значения, конституционные преобразования.

Интеграционные преобразования обусловлены рядом факторов, среди которых, как правило, называют следующие: исторический путь развития государственности, форма государства, традиции, политические и социально-экономические предпосылки, конституционная идентичность, идеология и правовая культура, национальные особенности, менталитет и специфика правовой коммуникации и иных коммуникационных процессов.

«В процессе становления и развития белорусского этноса его государственность нашла воплощение в виде исторических и национальных форм. Исторические формы государственности принадлежат не только белорусскому народу, но и другим народам (Полоцкая земля, Великое