коррупционных преступлений, с предоставлением полученных результатов ОРД инициатору[1].

Заслуживает интерес, хотя и не бесспорное, мнение профессора В.Н. Омелина, который, критикуя некоторые указанные выше предложения, пишет, что целесообразность внесения в ст. 7 ФЗ «Об ОРД» дополнительных оснований для проведения ОРМ по установлению имущества, подлежащему конфискации, можно поставить под сомнение. Обосновывая свою точку зрения тем, что имеющиеся в ст. 7 ФЗ «Об ОРД» основания, такие как наличие возбужденного уголовного дела, отдельное поручение следователя, можно отнести и к основаниям проведения ОРМ с целью установления имущества, подлежащего возможной конфискации[2].

Таким образом, необходимо тщательно подойти к правовой регламентации в теории ОРД оснований для проведения ОРМ с целью установления имущества, подлежащего конфискации. Представляется, что линия исследуемой оперативной работы в ходе осуществления ОРД должна быть четко прописана законодателем с целью исключения нарушения прав и законных интересов как граждан, попадающих в поле зрения органов, осуществляющих ОРД, так и потерпевших, чьи интересы в осуществлении правосудия носят ключевой характер.

Корниленко А.В.,

кандидат политических наук
Академия управления МВД России (г. Москва)

Оперативно-розыскное противодействие незаконному обороту персональных данных

Одним из приоритетных направлений деятельности подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий[3] является противодействие незаконному использованию и (или) передаче, сбору и (или) хранению компьютерной информации, содержащей персональные данные граждан.

[1] Шаров С.В. Установление имущества, добытого путем совершения коррупционных преступлений на стадии судебного процесса // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 1(53). С. 268-269.

[2] Омелин В.Н. Оперативно-розыскные меры по обеспечению возмещения имущественного ущерба, причиненного преступлениями // Вестник Владимирского юридического института. 2025. № 1(74). С.72.

[3] Далее – ИКТ.

Как известно, Федеральным законом от 30 ноября 2024 года № 421-ФЗ в Уголовный кодекс Российской Федерации[1] введена статья 272.1, предусматривающая уголовную ответственность за незаконные использование, передачу, сбор, хранение компьютерной информации, содержащей персональные данные, а равно создание, обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и распространения[2].

В федеральном законодательстве под персональными данными понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[3], а именно: фамилия, имя, отчество[4], дата рождения, место рождения, индивидуальный номер налогоплательщика, адрес, телефон, семейное положение, социальное положение, имущественное положение, образование, профессия, занимаемая должность, стаж работы, доходы и т. д.

Однако практика показывает, что критерием достаточности отнесения к персональным данным является наличие сведений, содержащих в себе как минимум два элемента, позволяющих косвенно идентифицировать лицо (например, Ф.И.О. и номер телефона, Ф.И.О. и дата рождения и т. д.).

При этом, по мнению прокуратуры России, ключевым условием наступления уголовной ответственности, предусмотренной статьей 272.1 УК РФ является одновременное наличие двух составляющих в действиях виновного лица:

1) незаконного способа завладения персональными данными в электронном виде;

2) незаконных действий, связанных с их распространением[5].

Учитывая, что действие указанной статьи не распространяется на случаи обработки персональных данных физическими лицами исключительно для личных и семейных нужд, особую сложность вызывает доказывание умысла причастных лиц, пытающихся уйти от ответственности. Также следует принимать во внимание ситуацию, когда действие (бездействие) формально хоть и содержит признаки какого-либо деяния, но в силу малозначительности не представляет общественной опасности и преступлением не является, что предусмотрено статьей 14 УК РФ.

Очевидно, что наибольшую общественную опасность представляют деяния, связанные именно с незаконным распространением персональных данных, и в первую очередь – с их продажей. Действия, связанные со сбором, хранением и использованием указанных данных, зачастую выступают в качестве вспо-

---

[1] Далее – УК РФ.

[2] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 30.11.2024 № 421-ФЗ // Собрание законодательства Российской Федерации, 2024. № 49 (часть IV). Ст. 7412.

[3] О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // Собрание законодательства Российской Федерации, 2006. № 31 (часть I). Ст. 3451.

[4] Далее – Ф.И.О.

[5] Разъяснения прокуратуры от 04.04.2025. URL: https://peredel-r40.gosweb.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti_17.html (дата обращения: 08.09.2025).

могательных составов при подготовке (совершении) иных преступлений и подлежат квалификации по совокупности с ними.

Несмотря на общее снижение количества интернет-ресурсов, связанных с неправомерным доступом к персональным данным (например, достаточно знаменитый ранее и уже недействующий сайт «Глаз Бога»), после введения уголовной ответственности, на сегодняшний день на территории Российской Федерации еще действует около 100 виртуальных площадок, предоставляющих такие услуги. По итогам 2024 года Роскомнадзором зафиксировано 135 случаев утечек данных, в которых содержалось более 710 млн записей о российских гражданах.

Собственно весь «теневой рынок» незаконного оборота персональных данных в настоящее время можно условно разделить на два основных сектора:

1. «Агрегаторы», собирающие и хранящие незаконно добытые персональные данные в соответствующих базах.

2. Сервисы «пробива», предоставляющие неправомерный доступ к персональным данным граждан из баз с ограниченным доступом.

Деятельность указанных интернет-площадок, представляется незаконной и может содержать в себе признаки правонарушений, предусмотренных как Кодексом Российской Федерации об административных правонарушениях (статьи 13.11, 13.14, 13.14.1), так и УК РФ (статьи 137, 138, 183, 272, 272.1, 273, 274, 274.1).

Данные деяния объединяет высокая степень латентности и уровень общественной опасности, основанной на «утечке» данных, составляющих тайну связи, банковскую, налоговую, коммерческую и иные виды тайн. Учитывая эти обстоятельства, наиболее оптимальным способом оперативно-розыскного противодействия представляется проведение оперативно-розыскного мероприятия[1] «Проверочная закупка», в отношении лиц, подозреваемых в незаконном обороте персональных данных.

Проведение указанного ОРМ позволяет достичь две цели:

1) задокументировать сам факт незаконного распространения охраняемой законом информации;

2) задокументировать умысел на совершение преступления (корыстную заинтересованность).

Следует отметить, что Министерством внутренних дел Российской Федерации прилагаются значительные усилия по нормативно-правовому, организационно-методическому обеспечению борьбы с данным видом преступности, а также обобщению и распространению правоприменительной практики среди подразделений по борьбе с киберпреступностью на региональном уровне.

[1] Далее – ОРМ.

Так, в марте – апреле текущего года МВД России был организован и проведен комплекс мероприятий по противодействию незаконному обороту персональных и иных охраняемых законом данных во всех субъектах Федерации. Проведение инициативных ОРМ позволило выявить канал «утечки» персональных данных клиентов кредитно-финансовой организации и привлечь к уголовной ответственности ее сотрудников по признакам состава преступления, предусмотренного частью 3 статьи 183 УК РФ.

Очевидно, что борьба с незаконным оборотом персональных данных носит комплексный характер и должна быть направлена на активное инициативное выявление лиц, событий и фактов, представляющих оперативный интерес в данной сфере деятельности.

Полуянов С.А.,

кандидат юридических наук
Тверской филиал Московского Университета МВД РФ им. В.Я. Кикотя (г. Тверь)

Сущность и некоторые аспекты содержания изъятия в оперативно-розыскной деятельности

Одной из задач оперативной разработки является документирование противоправных действий лиц, совершающих преступления. В оперативно-розыскной деятельности[1] традиционно выделяют три направления документирования[2]. Одно из них – выявление предметов и документов, которые могут быть доказательствами, и обеспечение возможности их использования в процессе расследования уголовного дела. Необходимость выявления предметов и документов вытекает из того, что они могут использоваться в качестве орудий при совершении преступлений, быть предметом преступного посягательства, содержать следы преступника, иметь запрет или ограничение в гражданском обороте, представлять иной интерес для оперативных подразделений органов внутренних дел. Выявленные предметы и документы, имеющие признаки доказательств преступной деятельности, относятся к фактическим данным, которые могут использоваться в качестве основы для формирования вещественных доказательств в уголовном процессе. Это обязывает сотрудников оперативных подразделений в процессе документирования не только выявлять предметы и документы, но и обеспечивать их сохранность до возбуждения уголовного дела для последующего приобщения к нему.

[1] Далее – ОРД.

[2] Оперативно-розыскная деятельность : учебник для студентов вызов / под науч. ред. Н.А. Кузьмина, Л.Л. Тузова; под общ. ред. Р.С. Тамаева, И.А. Климова. 10-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА, 2025. С. 311.