

УДК 343.3/.7

Юрышева Анастасия Николаевна*студент,**кафедра теории и истории государства и права,**Институт государственного права и национальной безопасности,**Байкальский государственный университет,**г. Иркутск, Российская Федерация,**e-mail: 0156747@bgu.ru*

СОБИРАНИЕ КАК СПОСОБ ПОЛУЧЕНИЯ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ, НАЛОГОВУЮ ИЛИ БАНКОВСКУЮ ТАЙНУ

Аннотация. В статье анализируется собирание как способ получения сведений, составляющих коммерческую, налоговую или банковскую тайну. Особое внимание уделяется признаку незаконности в контексте методов собирания информации. Также исследуется действующее законодательство, учебная и научная литература на предмет определения понятия «иной незаконный способ» собирания сведений. Отмечается несовершенство законодательной конструкции части 1 статьи 183 Уголовного кодекса РФ и предлагаются решения по совершенствованию законодательства в данной области.

Ключевые слова: статья 183 Уголовного кодекса, незаконное собирание сведения, коммерческая тайна, банковская тайна, налоговая тайна.

Anastasia N. Yurysheva*Student,**Department of Theory and History of State and Law,**Institute of State Law and National Security,**Baikal State University,**Irkutsk, Russian Federation,**e-mail 0156747@bgu.ru*

COLLECTION AS A WAY OF OBTAINING INFORMATION COMMERCIAL, TAX OR BANKING SECRECY

Abstract. The article analyses collection as a method of obtaining information constituting commercial, tax or banking secrecy. Particular attention is paid to the sign of illegality in the context of information gathering methods. The current legislation, academic and scientific literature on the definition of the concept of «other illegal way» of collecting information is also studied. The imperfection of the legislative construction of part 1 of article 183 of the Criminal Code of the Russian Federation is noted and solutions to improve the legislation in this area are proposed.

Keywords: article 183 of the Criminal Code, unlawful collection of information, commercial secret, bank secrecy, tax secrecy.

В условиях современности, когда информация является одним из ключевых и ценных ресурсов, вопросы защиты конфиденциальности данных имеют особую актуальность. В частности, такие виды информации, как коммерческая, налоговая или банковская тайна, нередко становятся объектом противоправных действий. Уголовное законодательство, а именно ст. 183 УК РФ), охраняет данную сферу деятельности и устанавливает ответственность за незаконное получение указанных сведений. Но при этом формулировка ч. 1 диспозиции данной статьи представляется неясной, в связи с чем на практике возникают проблемы ее применения. В рамках данной статьи будет рассмотрен такой способ получения сведений, составляющих коммерческую, налоговую или банковскую тайну, как собирание. При этом анализ того, что представляет собой незаконное собирание сведений, является очень сложным юридическим вопросом. Это связано с тем, что законодатель не дает никаких дополнительных разъяснений относительно того, что именно является незаконным собиранием сведений. По этой причине не совсем ясно, как именно толковать норму, предусмотренную ч. 1 ст. 183 УК РФ, и как грамотно применять ее на практике. Во-первых, данное действие может быть осуществлено большим количеством способов, особенно с учетом развития информационных технологий, значительно расширяющих возможности совершения указанного деяния. А диспозиция указанной нормы закрепляет только несколько из них и порождает юридическую неопределенность размытой формулировкой «иным незаконным способом». Во-вторых, не установлено никаких критериев, как именно оценивать незаконность данных методов.

В рамках научного анализа понятия «незаконность» необходимо учитывать следующие ключевые факторы.

1. Критерии, определяющие незаконные действия с точки зрения действующих норм. Любые действия, противоречащие действующему законодательству и нарушающие права и интересы граждан и организаций следует считать незаконными. Также в контексте охраны отношений в экономической и финансовой сферах деятельности к незаконным действиям следует относить те, которые нарушают нормы профессиональной этики.

2. Конфиденциальный характер сведений, на которые направлено преступление. Информация, которая является предметом преступления, должна носить конфиденциальный характер, то есть иметь ограниченный доступ. В соответствии со ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» под конфиденциальностью информации понимается «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя» [1]. Обычно такие требования прямо закрепляются в нормативных актах или учредительных документах организации. К конфиденциальным сведениям могут относиться данные о финансовых операциях, бухгалтерские отчеты, личная информация клиентов и т. д. Поэтому для понимания незаконного собирания сведений необходимо обращаться к вышеуказанным документам.

3. Анализ конкретных технологий и методов, использование которых следует квалифицировать как незаконное. В данном аспекте, прежде всего, следует понимать различия между законными методами сбора информации, которые соответствуют нормативным правовым актам (например, поиск информации в открытых источниках неограниченного доступа) и теми, которые нарушают конфиденциальность информации и влекут за собой нарушение прав граждан и интересов организаций. Во-вторых, учитывая стремительно развивающиеся цифровые технологии, законодательство должно также быстро адаптировать нормы в целях грамотного регулирования данной сферы. То есть при анализе конкретного метода следует обращаться не только к уголовному законодательству, но и к другим правовым актам, содержащим стандарты информационной безопасности.

Некоторые исследователи полагают, что признак незаконности в контексте понимания ст. 183 УК РФ должен быть определен не только объективной противоправностью, ключевые моменты которой описаны выше, но и субъективной, предполагающей установление того, что лицо, совершившее незаконное собирание сведений, «не имело ни действительного, ни предполагаемого права на применение данного способа и осознает это» [2, с. 179]. Если обратиться к нормативным актам, регулирующим конфиденциальность коммерческой, налоговой и банковской информации, то можно отметить, что законодатель придерживается этой позиции по данному вопросу. Так, в ст. 4 ФЗ «О коммерческой тайне» указано, что «информация, составляющая коммерческую тайну, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, и что лицо не имеет на передачу этой информации законного основания» [3].

Таким образом, вопрос признака незаконности в контексте применения ст. 183 УК РФ можно считать в какой-то мере урегулированным законодательством. Вместе с тем важно отметить необходимость его непрерывного совершенствования в отношении регулирования новых технических методов собирания информации. Эпоха цифровизации и технологического прогресса требует адекватного и гибкого правового регулирования для обеспечения защиты конфиденциальных данных и предотвращения их незаконного использования. Значит, несмотря на определенный уровень законодательной базы, вопрос остается открытым и требует постоянного внимания со стороны законодателя, правоприменителя и научного сообщества.

Вернемся к проблеме понимания формулировки ч. 1 ст. 183 УК РФ в части определения иного способа незаконного собирания информации. Отсутствие по этому поводу разъяснений со стороны Верховного Суда РФ оставляет неопределенность в этом вопросе, что порождает проблемы при квалификации деяний и неоднородную судебную практику. Учеными подчеркивается необходимость точного формулирования законодательных норм, важность четкого определения

границ уголовно-наказуемых деяний для избежания правовой неопределенности, обеспечения прозрачности правоприменения, справедливого правосудия и гарантии прав граждан [4, с. 78; 5, с. 18].

Учеными неоднократно предпринимались попытки по выработке позиции относительно того, что именно следует понимать под «иным незаконным способом» собирания сведений и какие деяния следует квалифицировать в соответствии с данным способом. Так, к иному способу собирания сведений предлагается относить неправомерный доступ к компьютерной информации, применение устройств и средств, предназначенных для негласного сбора информации, неправомерный доступ к компьютерной информации, а также поиск, сбор, фиксация сведений в нарушение режима доступа к такой информации [6, с. 487]. Полагаем, такой подход внесет некоторую ясность в уточнение и конкретизацию данного аспекта уголовного закона. Вместе с тем стоит указать на определенные ограничения данного понятия такой трактовкой, как предполагающей слишком строгое фокусирование на определенных действиях в сфере неправомерного доступа к информации без учета всех возможных сценариев незаконного сбора информации, особенно в условиях быстро меняющихся технологий и методов обработки данных. К тому же подобное определение иного способа собирания сведений через призму данных действий может создать коллизию со ст. 272 УК РФ, которая прямо регулирует данную сферу деятельности.

Также некоторые ученые пытаются более конкретно описать действия, которые входят в понятие «иные незаконные способы собирания сведений», перечисляя отдельные технические методы [7, с. 61]. В их число входят: взлом компьютерных систем; использование вредоносного ПО; фишинг; перехват сетевого трафика; скрытое прослушивание и видеонаблюдение; использование ложных сетевых узлов; расшифровка данных и т. д. Но, как отмечалось, цифровые технологии постоянно совершенствуются, появляются новые инновационные средства, что влечет за собой эволюцию и способов совершения преступления. Причем это происходит столь стремительно, что невозможно проследить их появление, поэтому попытка простого перечисления возможных способов незаконного собирания информации является неудачной, поскольку в полном объеме сделать это вряд ли возможно.

Ряд исследователей придерживается идеи о необходимости просто указать универсальные признаки деяний, которые входят в данное понятие. По их мнению, иное незаконное собирание сведений включает в себя «любые действия в виде поиска, отбора, фиксации, обработки, накопления или хранения сведений, совершенные с нарушением режима доступа к такой информации» [8, с. 146]. Однако данный подход представляется не совсем удачным в рамках точного и эффективного правоприменения. Во-первых, уяснение понятия через его универсальные признаки приводит к слишком широкому толкованию и, как следствие, к правовой неопределенности. Определение общих критериев без конкретизации контекста и специфики может предоставить некоторую свободу действий при применении закона в разных регионах страны, что не соответствует принципам законности, справедливости и равенства всех перед законом. Во-вторых, такой

подход может привести к неправильной оценке обстоятельств при совершении каждого отдельного случая незаконного собирания сведений. Применение норм уголовного закона должно учитывать не только формальное выполнение или несоблюдение определенных процедур, но и конкретные обстоятельства, при которых совершено деяние, включая мотивы, цели и последствия действий. Третья причина кроется в непрерывном развитии научно-технического прогресса, в ходе которого могут появиться новые методы, не подпадающие под указанные признаки. Несмотря на то, что такой теоретический подход ученых кажется простым и универсальным, на практике он может привести к еще большим трудностям.

Некоторые ученые предлагают вовсе исключить формулировку «иным незаконным способом» из диспозиции ч. 1 ст. 183 УК РФ, чтобы избежать неопределенности в правоприменении [9, с. 128]. Но это также может привести к ряду сложностей. В частности, такой подход существенно ограничит возможности законодателя по реагированию на новые методы собирания информации. На наш взгляд, все-таки необходимо поддерживать баланс между строгой юридической определенностью и ее полным отсутствием.

В последнее время также набирает популярность предложение, согласно которому следует выделить исчерпывающий перечень наиболее опасных методов собирания информации и включить их в диспозицию ч. 1 ст. 183 УК РФ [10, с. 160]. Такой подход также подвергается критике. Во-первых, выбор определенных методов и их законодательное закрепление может ограничить с юридической точки зрения объективную сторону данного состава преступления. В связи с этим многие другие методы, которые успешно используются для совершения данного преступления, могут оказаться за рамками правового поля, что позволит виновному лицу избежать ответственности. Второй момент опять же связан с непрерывным развитием технического прогресса. И самый существенный недостаток этого подхода: по каким критериям следует определять степень общественной опасности каждого метода?

В связи с большим количеством различных точек зрения по данному вопросу требуется выработка наиболее универсального подхода, который бы включал преимущества каждой из вышеуказанных теорий. Поэтому представляется целесообразным внести предложение по выработке разъяснения Верховного Суда РФ о практике применения ст. 183 УК РФ. Данное разъяснение должно закрепить конкретные указания по применению части 1 данной нормы с учетом развития информационных технологий. В постановлении следует указать часто встречающиеся на практике методы незаконного собирания, а также рассмотреть требования по квалификации методов, которые ранее не имели практики по их регулированию. Это обеспечит юридическую ясность, поможет избежать правовой неопределенности, будет способствовать формированию единой и последовательной судебной практики.

Список использованной литературы

1. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июня 2006 г. № 149-ФЗ (ред. от 12 ноября 2023 г.) // СЗ РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.
2. Клебанов Л. Р. Незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну: особенности квалификации / Л. Р. Клебанов // Вестник Омского университета. – 2014. – № 2 (39). – С. 178–183.
3. О коммерческой тайне : Федеральный закон от 29 июля 2004 г. № 98-ФЗ (ред. от 14 июля 2022 г.) // СЗ РФ. – 2004. – № 32. – Ст. 3283.
4. Кобзева Е. В. Идеологические и правовые границы российского уголовного закона: о необходимости их выделения и соблюдения / Е. В. Кобзева // Вестник СГЮА. – 2014. – № 5 (100). – С. 75–78.
5. Корнакова С. В. К вопросу о факторах, влияющих на формирование доверия общества к суду и правосудию / С. В. Корнакова // Российский судья. – 2020. – № 1. – С. 14-19.
6. Уголовное право. Общая и Особенная части : учебник / под общ. ред. М. П. Журавлева и С. И. Никулина. – М., 2014. – 784 с.
7. Петроченков С. Д. Квалификация способов совершения преступления, предусмотренного статьей 183 УК РФ / С. Д. Петроченков // Юрист-Правоведъ. – 2017. – № 1 (80). – С. 59–62.
8. Шутова А. А. Незаконное собирание сведений, составляющих коммерческую или банковскую тайну, путем подкупа: проблемы правоприменения / А. А. Шутова // Вестник Российского университета кооперации. – 2017. – № 3 (29). – С. 143–148.
9. Ефремова М. А. Уголовно-правовая охрана сведений, составляющих коммерческую, налоговую и банковскую тайны / М. А. Ефремова // Вестник Пермского университета. – 2015. – № 1. – С. 124–132.
10. Карташов С. В. Современные проблемы квалификации незаконных получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну, связанные с толкованием отдельных признаков составов преступлений / С. В. Карташов // Вестник Московского университета МВД России. – 2017. – № 5. – С. 159–167.