

Научная статья

<https://doi.org/10.24412/2658-7335-2026-3-11>

УДК: 343.3/7



Attribution

cc by

СВЕДЕНИЯ О СОЕДИНЕНИЯХ И ГЕОЛОКАЦИИ В ЧАСТНОЙ ДЕТЕКТИВНОЙ
ДЕЯТЕЛЬНОСТИ: УГОЛОВНО-ПРАВОВАЯ ОЦЕНКА

Швецов Р.Е.

Российский университет адвокатуры и нотариата имени Г. Б. Мирзоева

Аннотация. Цель статьи — определить критерии уголовно-правовой оценки получения частным детективом сведений о телефонных соединениях, базовых станциях, местоположении абонентского устройства и иных данных связи. Методологическую основу исследования составили формально-юридический, системный и правоприменительный методы, а также выборочный анализ судебных ситуаций, связанных с незаконным получением телекоммуникационных сведений. Обосновывается, что такие сведения не являются обычным результатом наведения справок в частной сыскной деятельности, поскольку затрагивают тайну связи, персональные данные и компьютерную информацию. Сделан вывод, что квалификация зависит от вида сведений, способа доступа, роли инсайдера, передачи результата заказчику и профессионального контекста; возможна оценка по ст. 138, 272, 272.1 и 203 УК РФ.

Ключевые слова: частный детектив, частная сыскная деятельность, тайна связи, сведения о соединениях, геолокация, персональные данные, компьютерная информация, ст. 138 УК РФ, ст. 203 УК РФ.

Финансирование: инициативная работа.

Original article

CONNECTION AND GEOLOCATION DATA IN PRIVATE DETECTIVE ACTIVITY:
CRIMINAL LAW ASSESSMENT

Roman E. Shvetsov

G. B. Mirzoev Russian University of Advocacy and Notariat

Abstract. The purpose of the article is to define criteria for criminal law assessment of a private detective's obtaining of connection data, base-station information, location of a subscriber device and other communication data. The methodology includes formal legal, systemic and law-enforcement methods, as well as selective analysis of court situations involving unlawful access to telecommunication information. The article substantiates that such data cannot be treated as an ordinary result of making inquiries in private investigative activity, since they affect secrecy of communications, personal data and computer information. It is concluded that qualification depends on the type of data, method of access, role of an insider, transfer of the result to the client and professional context; assessment under Articles 138, 272, 272.1 and 203 of the Criminal Code may be required.

Keywords: private detective, private investigative activity, secrecy of communications, connection data, geolocation, personal data, computer information, Article 138, Article 203.

Funding: Independent work.

Введение.

Частная детективная деятельность по своей социальной природе связана с поиском, проверкой и передачей информации заказчику. Именно поэтому в практической плоскости одним из наиболее востребованных, но одновременно наиболее рискованных направлений незаконного частного сыска становится получение сведений о телефонных соединениях, базовых станциях и местоположении абонентского устройства. Заказчик нередко воспринимает такую информацию как обычный результат «проверки», «поиска» или «наведения справок», однако правовой режим этих сведений существенно отличается от режима открытой информации.

Сведения о телефонных соединениях, абонентских номерах, времени, длительности и направлении коммуникаций, а также данные о базовых станциях и примерном местоположении устройства позволяют восстановить круг общения, маршруты

перемещения, семейные, деловые и социальные связи лица. В этом смысле речь идёт не о нейтральной справочной информации, а об информационном массиве, способном раскрывать значимые элементы частной жизни и коммуникационного поведения человека.

Центральная проблема состоит в том, что сведения о соединениях и местоположении абонентского устройства внешне могут восприниматься заказчиком как обычный информационный результат детективной услуги, однако по своему правовому режиму они относятся к охраняемой информации и не могут быть получены частным детективом вне предусмотренных законом процедур. Законная частная сыскная деятельность не предоставляет частному детективу права требовать у операторов связи детализацию, сведения о базовых станциях, биллинговые данные или геолокацию абонента.

Цель настоящей статьи состоит в определении критериев уголовно-правовой оценки получения частным детективом сведений о соединениях и геолокации.

Предметом исследования выступают уголовно-правовые и информационно-правовые нормы, регулирующие охрану тайны связи, персональных данных, компьютерной информации и пределы частной сыскной деятельности.

Методологически исследование основано на формально-юридическом анализе уголовно-правовых и информационно-правовых норм, системном сопоставлении режимов тайны связи, персональных данных и компьютерной информации, а также на выборочном анализе судебных ситуаций по критериям предметной связи с получением телекоммуникационных сведений, периода выявления проблемы в судебной практике и значения для разграничения ст. 138, 137, 272, 272.1 и 203 УК РФ, связанных с незаконным получением телекоммуникационных сведений.

Научная новизна статьи состоит в предложении специального критерия квалификации: учитывать не только статус частного детектива, но и вид сведений, способ доступа, наличие служебного доступа у источника, профессиональную связь с детективным поручением, передачу результата заказчику и самостоятельность охраняемых объектов.

Полученные выводы могут быть использованы при квалификации деяний частных детективов, связанных с получением телекоммуникационных сведений, а также при разработке разъяснений судебной практики о соотношении ст. 138, 272, 272.1 и 203 УК РФ.

Эмпирическая база исследования уточняется как выборочная: в неё включены судебные ситуации, в которых фигурируют получение детализации телефонных соединений, использование операторских или иных закрытых информационных ресурсов, а также профессиональная связь таких действий с частной сыскной деятельностью. Эти материалы используются не как статистическая выборка, а как правоприменительные примеры, демонстрирующие типовые квалификационные затруднения и неоднородность подходов к оценке телекоммуникационных сведений.

Результаты.

Сведения о соединениях и геолокации как предмет незаконного интереса заказчика.

В частной детективной практике незаконный интерес заказчика к сведениям связи обычно имеет прикладной характер. Заказчика интересует не абстрактная тайна связи, а конкретный результат: с кем общается лицо, когда и как часто происходят соединения, где находилось абонентское устройство, какие маршруты можно восстановить по базовым станциям, с какими абонентами поддерживалась регулярная связь. Такие сведения могут запрашиваться в семейных, имущественных, корпоративных, долговых, конкурентных или личных конфликтах.

К типичным объектам незаконного интереса относятся входящие и исходящие соединения, номера абонентов, дата, время и длительность звонков, сведения о фактах отправки и получения SMS-сообщений, данные о базовых станциях, примерное местоположение телефона, история перемещения абонентского устройства, а иногда и сопутствующие сведения об абоненте. Даже если содержание разговора или сообщения не раскрывается, сам факт, интенсивность, частота и направление коммуникации имеют самостоятельное информационное значение.

Опасность незаконного получения сведений о соединениях состоит не только в раскрытии факта коммуникации, но и в возможности построить социальный, семейный, деловой или пространственный профиль лица. По детализации телефонных соединений можно установить круг общения, частоту контактов, периодичность взаимодействия с определёнными лицами, косвенные признаки семейного конфликта, деловой активности или передвижения. Данные базовых станций и геолокации позволяют реконструировать перемещения, сопоставлять местонахождение лица с событиями, встречами или иными обстоятельствами.

Такие сведения обычно невозможно получить законно в рамках обычной частной детективной услуги. Поэтому в незаконной практике они добываются через работников операторов связи, бывших сотрудников, посредников, лиц, имеющих доступ к биллинговым системам, нелегальные цифровые сервисы, Telegram-боты или иные неформальные каналы. Потерпевший, как правило, не знает о сборе таких сведений и не может своевременно воспрепятствовать их передаче заказчику.

Именно латентность делает подобные деяния особенно опасными. Лицо может узнать о незаконном сборе сведений только после того, как информация уже использована в споре, конфликте, переговорах, бракоразводном процессе, корпоративной борьбе или иной ситуации давления. Поэтому уголовно-правовая оценка получения сведений о соединениях и геолокации должна строиться не по бытовому восприятию такой услуги заказчиком, а по правовому режиму полученной информации и способу доступа к ней.

Следует учитывать, что официальная уголовная статистика обычно не выделяет незаконное получение детализации соединений и геолокационных данных частными детективами в самостоятельную категорию. Поэтому вывод о латентности таких деяний основан на их способе совершения: сведения добываются через закрытые информационные каналы, передаются заказчику без уведомления проверяемого лица и обнаруживаются преимущественно тогда, когда уже использованы в конфликте. Такая конструкция снижает вероятность своевременного выявления потерпевшим самого факта вмешательства.

Пределы законного частного сыска: почему детализация и геолокация не являются «наведением справок».

Закон РФ № 2487-1 допускает осуществление частной детективной деятельности в строго определенных пределах. Частный детектив вправе оказывать предусмотренные законом сыскные услуги, проводить устный опрос с согласия граждан, наводить справки, изучать предметы и документы с согласия их владельцев, осуществлять внешний осмотр и наблюдение в допустимых законом рамках¹. Однако эти полномочия не означают права доступа к закрытым информационным ресурсам операторов связи.

Наведение справок в частной сыскной деятельности не может толковаться как право на получение данных оператора связи, поскольку лицензия частного детектива не создаёт публичного или служебного информационного доступа. Частный детектив не вправе требовать у оператора связи детализацию телефонных соединений, сведения о базовых станциях, данные о местоположении абонентского устройства или иную информацию, доступ к которой ограничен законом. Получение таких сведений через работника оператора, посредника или нелегальный цифровой сервис не является реализацией права на наведение справок, а представляет собой обход установленного правового режима. Иное возможно только при наличии надлежащего правового основания, например, волеизъявления самого абонента в предусмотренной законом форме, однако поручение третьего лица само по себе такого основания не создаёт.

Согласие самого абонента или субъекта персональных данных должно быть конкретным, осознанным и относиться именно к тому объёму сведений, который предполагается получить и передать. Общее согласие на проверку, бытовое согласие в переписке либо согласие, данное третьему лицу без указания оператора, периода, вида данных и цели обработки, не должно рассматриваться как достаточное основание для получения детализации соединений или геолокационных сведений. Для уголовно-правовой оценки это означает, что наличие согласия подлежит специальной проверке: если согласие отсутствует, сфальсифицировано, получено обманом либо не охватывает спорный объём данных, деяние сохраняет признаки незаконного доступа к охраняемой информации.

Федеральный закон «О связи» прямо гарантирует на территории Российской Федерации тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и почтовой связи, а

ограничение этого права допускается только в случаях, предусмотренных федеральными законами². Следовательно, сведения, связанные с коммуникацией абонента, находятся в специальном правовом режиме. Частный детектив не включён в число субъектов, которым предоставляется публичное право ограничивать тайну связи.

Кроме того, сведения о соединениях и местоположении абонентского устройства могут содержать персональные данные, поскольку позволяют прямо или косвенно идентифицировать лицо, его контакты, поведение и перемещения. Федеральный закон «О персональных данных» направлен на защиту прав и свобод человека при обработке персональных данных, включая защиту права на неприкосновенность частной жизни, личную и семейную тайну³. Поэтому незаконное получение и передача таких сведений не могут рассматриваться только как нарушение договорной или лицензионной дисциплины частного детектива.

Особое значение имеет запрет на осуществление оперативно-розыскных действий частными детективами. Федеральный закон «Об оперативно-розыскной деятельности» связывает оперативно-розыскные мероприятия с деятельностью уполномоченных государственных органов⁴. Частный детектив не вправе подменять такие органы и использовать каналы получения сведений, характерные для публичного расследования. Если сведения о соединениях или геолокации добываются через результаты оперативно-розыскной деятельности, служебные базы или инсайдеров, это не расширяет полномочия частного детектива, а усиливает противоправный характер получения информации.

Таким образом, детализация телефонных соединений и геолокация не являются разновидностью обычной справки. Они связаны с тайной связи, персональными данными и режимом ограниченного доступа к информационным системам оператора. Поэтому квалификация их незаконного получения должна строиться не через категорию допустимого частного сыска, а через анализ уголовно охраняемых информационных объектов.

Уголовно-правовая оценка незаконного получения сведений о связи.

Незаконное получение сведений о соединениях не имеет единой квалификации: она зависит от правового режима сведений, способа доступа к ним и того, причинён ли вред тайне связи, частной жизни, компьютерной информации или персональным данным. В одних случаях центральным объектом будет тайна связи, в других — компьютерная информация, в-третьих — персональные данные или частная

¹Закон Российской Федерации от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» // Ведомости СНД РФ и ВС РФ. 1992. № 17. Ст. 888. Ст. 3, 5, 7.

²Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства РФ. 2003. № 28. Ст. 2895. Ст. 63.

³Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 2006. № 31, ч. 1. Ст. 3451. Ст. 2, 3.

⁴Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. 1995. № 33. Ст. 3349. Ст. 1, 6, 13.

жизнь. Поэтому правоприменитель не должен механически выбирать одну норму только потому, что речь идёт о телефонной детализации.

Первым возможным направлением оценки является ст. 138 УК РФ, предусматривающая ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений⁵. В литературе подчёркивается, что уголовно-правовая охрана тайны сообщений направлена не только на защиту содержания коммуникации, но и на недопустимость произвольного доступа к коммуникационной сфере лица [1; 2]. Сведения о соединениях могут раскрывать сам факт коммуникации, круг адресатов, время и интенсивность контактов. Поэтому при незаконном получении таких сведений необходимо проверять, затронут ли режим тайны связи.

Вместе с тем, сведения о соединениях требуют самостоятельного обоснования как предмета уголовно-правовой охраны. Содержание телефонного разговора или сообщения и сведения о факте, времени, продолжительности, направлении соединения, используемой базовой станции либо маршруте абонентского устройства не совпадают по фактическому содержанию. Однако в конституционно-правовом и уголовно-правовом смысле тайна связи не должна сводиться только к содержанию переговоров: охране подлежит и сама коммуникационная сфера лица, поскольку данные о контактах позволяют выявить круг общения, интенсивность взаимодействия и социальные связи. Поэтому вопрос о ст. 138 УК РФ должен решаться не автоматически, а через проверку того, нарушен ли режим конфиденциальности коммуникации и были ли сведения получены вне предусмотренной законом процедуры.

Вторым направлением является ст. 137 УК РФ. Сама по себе, детализация соединений не всегда раскрывает частную жизнь в содержательном смысле. Однако в сочетании с иными сведениями, с анализом круга общения, семейных связей, маршрутов перемещения или личных обстоятельств она может становиться средством вмешательства в частную жизнь. Если полученные данные используются для установления личных отношений, семейного поведения, интимных обстоятельств, скрытых контактов или иного приватного профиля лица, возникает вопрос о посягательстве на неприкосновенность частной жизни [3].

Критерием перехода от нарушения тайны связи к посягательству на частную жизнь является не сам технический факт получения детализации, а её содержательное использование для реконструкции личной сферы. Если сведения о соединениях ограничиваются фактом незаконного доступа к коммуникационным данным, основной акцент делается на тайне связи. Если же они сопоставляются с адресами, маршрутом, семейным положением, местом работы,

кругом близких лиц, встречами или иными обстоятельствами, позволяющими создать поведенческий профиль лица, возникает дополнительная проверка признаков ст. 137 УК РФ. Такой подход позволяет избежать расширительного толкования и одновременно не оставлять без оценки случаи, когда телекоммуникационные сведения становятся инструментом вторжения в частную жизнь.

Третьим направлением является ст. 272 УК РФ. Если сведения о соединениях получены через неправомерный доступ к информационной системе оператора связи, биллинговой базе, служебному интерфейсу или иной компьютерной системе, необходимо оценивать содеянное с точки зрения неправомерного доступа к компьютерной информации⁶. В таком случае предметом посягательства является не только коммуникационная тайна, но и охраняемая законом компьютерная информация, находящаяся в информационной системе оператора [4; 5].

Четвёртым направлением является ст. 272.1 УК РФ, введённая для защиты компьютерной информации, содержащей персональные данные⁷. Если сведения о соединениях, абонентских данных, местоположении устройства или иной телекоммуникационной информации обрабатываются в компьютерной форме и содержат персональные данные, незаконное использование, передача, сбор или хранение таких данных могут требовать самостоятельной оценки. Особенно это значимо при массовой выгрузке данных, передаче сведений третьим лицам или использовании цифровых ресурсов для их незаконного оборота [6].

При применении ст. 272.1 УК РФ необходимо учитывать её самостоятельную конструкцию. Неправомерный доступ к информационной системе оператора связи прежде всего оценивается через ст. 272 УК РФ, тогда как ст. 272.1 УК РФ требует проверки незаконных действий именно с компьютерной информацией, содержащей персональные данные: её сбора, хранения, передачи, распространения либо иного оборота. Поэтому получение работником оператора сведений из биллинговой системы, последующая выгрузка массива персональных данных, передача такого массива частному детективу и последующее предоставление результата заказчику могут образовывать разные юридически значимые этапы. В зависимости от фактической роли участников следует разграничивать неправомерный доступ, незаконный оборот персональных данных и использование полученного результата в рамках детективного поручения.

Если получение сведений о связи сопровождается использованием специальных технических средств, предназначенных для негласного получения информации, дополнительно возникает вопрос о самостоятельном уголовно-правовом режиме таких средств [7].

⁵Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954. Ст. 138.

⁶Уголовный кодекс Российской Федерации. Ст. 272.

⁷Уголовный кодекс Российской Федерации. Ст. 272.1.

Статья 183 УК РФ обычно не является основной нормой для оценки операторской детализации абонента, если речь идёт о частной коммуникации физического лица. Однако она может приобретать значение, когда незаконно полученные сведения связаны с коммерческой тайной организации, корпоративными переговорами, деловыми контактами, клиентской базой или иными сведениями, имеющими коммерческую ценность [8]. В таких случаях квалификация зависит не от самого факта телекоммуникационного канала, а от режима охраняемой тайны, к которой относятся сведения.

Следовательно, незаконное получение сведений о связи требует многослойной уголовно-правовой оценки. Статья 138 УК РФ отвечает за тайну коммуникации, ст. 137 УК РФ — за частную жизнь, ст. 272 УК РФ — за неправомерный доступ к компьютерной информации, ст. 272.1 УК РФ — за незаконное обращение с компьютерной информацией, содержащей персональные данные. Вопрос о ст. 203 УК РФ возникает дополнительно, если деяние связано с профессиональным частным сыском.

Обсуждение.

Служебный доступ оператора связи и статус частного детектива.

Особое значение для квалификации имеет вопрос о том, кто именно обладал доступом к сведениям о соединениях. Работник оператора связи или иное лицо, имеющее доступ к биллинговым системам, карточкам абонентов, детализациям и техническим данным, может использовать служебные возможности для незаконной выгрузки сведений. В таком случае его действия могут оцениваться с учётом служебного положения, если соответствующий квалифицирующий признак предусмотрен применимой уголовно-правовой нормой.

Частный детектив находится в иной позиции. Его лицензия на осуществление частной детективной деятельности не предоставляет доступа к информационным системам оператора связи. Если он получает сведения через работника оператора, бывшего сотрудника, посредника или иное лицо, то использует не служебный доступ, а профессиональные связи, заказ, оплату, репутацию или организационную роль в получении результата. Поэтому служебный доступ к сведениям о соединениях имеет работник оператора связи или иной обладатель доступа, но не частный детектив, если его статус основан только на лицензии частного сыщика.

Это различие важно для разграничения ролей. Работник оператора связи может быть исполнителем незаконного доступа или передачи сведений, если именно он использует служебные возможности. Частный детектив может выступать организатором, пособником, подстрекателем, приобретателем результата или самостоятельным исполнителем иного состава — в зависимости от фактической модели деяния. Заказчик, в свою очередь, может нести ответ-

ственность при наличии умысла на незаконное получение сведений и соответствующего вклада в совершение преступления.

В научной литературе по ст. 203 УК РФ обращается внимание на необходимость точного установления субъективных и статусных признаков при квалификации превышения полномочий [9; 10]. Применительно к сведениям связи это означает, что нельзя автоматически переносить признак служебного положения с работника оператора на частного детектива. Если детектив не обладает служебным доступом к системе оператора, его повышенная опасность выражается не в службе, а в профессиональном использовании частного сыска для получения закрытых сведений.

Судебные ситуации, связанные с незаконной передачей детализации через работников операторов связи, подтверждают эту логику. В таких делах служебный доступ относится к лицу, имеющему техническую или должностную возможность получить сведения из системы оператора, тогда как роль внешнего получателя определяется отдельно: через заказ, оплату, посредничество, передачу результата и осознание незаконности источника. Поэтому квалификация должна строиться не по абстрактному статусу частного детектива, а по тому, какое действие он совершил и какой информационный режим был нарушен.

В настоящей статье такие судебные ситуации используются выборочно, поскольку они иллюстрируют не статистическую распространённость, а юридически значимые модели поведения: наличие инсайдера с доступом к операторской или иной закрытой системе, передачу результата внешнему получателю, профессиональное использование сведений частным детективом и последующее применение информации заказчиком. Именно эти признаки имеют значение для разработки критериев квалификации и позволяют отделить бытовой незаконный доступ к информации от профессионального информационного злоупотребления.

Соотношение ст. 138, 272, 272.1 и 203 УК РФ.

Если сведения о соединениях получены обычным лицом вне связи с частной сыской деятельностью, ст. 203 УК РФ не применяется. В такой ситуации правоприменитель должен оценивать признаки специальных информационных составов и возможное соучастие. Иная ситуация возникает, когда сведения получает лицензированный частный детектив в рамках поручения заказчика, за вознаграждение, с подготовкой отчёта или передачей результата как продукта детективной услуги.

Статьи 138, 272 и 272.1 УК РФ оценивают конкретный информационный объект. Статья 138 УК РФ защищает тайну связи; ст. 272 УК РФ — охраняемую компьютерную информацию; ст. 272.1 УК РФ — компьютерную информацию, содержащую персональные данные. Статья 203 УК РФ имеет иной фо-

кус: она позволяет поставить вопрос о профессиональном выходе частного детектива за пределы дозволенной частной сыскной деятельности. Поэтому при профессиональном контексте незаконное получение сведений о соединениях может требовать не только оценки нарушения тайны связи или компьютерной информации, но и проверки признаков превышения полномочий частным детективом.

Такая совокупность не является автоматической. Необходимо установить, что лицо имело статус частного детектива; деяние было связано с выполнением или имитацией выполнения детективного поручения; конкретное поведение выходило за пределы разрешённых законом способов частного сыска; наступило существенное нарушение прав; а также имеются признаки соответствующего информационного состава. Если хотя бы один из этих элементов отсутствует, применение ст. 203 УК РФ может быть необоснованным.

В деле Савеловского районного суда г. Москвы незаконное получение детализации телефонных соединений было связано с обращением к частному детективу, оплатой услуги и передачей результата заказчику. Содеянное получило оценку по совокупности ст. 203 УК РФ и специальных информационных составов⁸. Это показывает, что профессиональная форма получения телекоммуникационных сведений может иметь самостоятельное значение наряду с нарушением тайны связи или частной жизни.

Иной пример демонстрирует дело Дикушина, где фигурировали сведения о телефонных соединениях, налоговые и банковские данные, а также обстоятельства, указывавшие на профессиональный контекст частной детективной деятельности. Однако суд исключил ст. 203 УК РФ как излишнюю⁹. Это дело показывает не отсутствие проблемы, а необходимость чётких критериев разграничения: наличие информационного состава не должно автоматически исключать оценку профессионального превышения, но и ст. 203 УК РФ не должна применяться без установления самостоятельного вреда порядку частного сыска.

Следовательно, если незаконное получение сведений о соединениях совершено частным детективом в рамках детективного поручения, правоприменитель должен оценивать не только нарушение тайны связи или компьютерной информации, но и возможный профессиональный выход за пределы частной сыскной деятельности. При этом совокупность допустима только при самостоятельности охраняемых объектов.

Критерии квалификации.

Квалификация получения частным детективом сведений о соединениях и геолокации должна строиться не по названию услуги и не по статусу за-

казчика, а по правовому режиму полученных сведений, способу доступа и профессиональной роли частного детектива. Для этого можно выделить несколько критериев.

Первый критерий — вид сведений. Необходимо установить, что именно было получено: содержание сообщений, сведения о соединениях, абонентские данные, данные о базовых станциях, местоположение абонентского устройства, история перемещения, сведения о владельце номера или массив персональных данных. Разные виды сведений могут затрагивать разные уголовно охраняемые объекты. При этом вид сведений следует оценивать не формально, а функционально. Данные о соединениях и геолокации могут выступать самостоятельным объектом тайны связи, но при сопоставлении с иными данными они способны приобретать качество сведений о частной жизни. Поэтому квалификация должна учитывать не только источник данных, но и то, какой информационный профиль лица фактически сформирован в результате их получения и передачи.

Второй критерий — способ доступа. Открытый источник, добровольное предоставление информации самим лицом, законное согласие, запрос к оператору, использование инсайдера, доступ к базе оператора, Telegram-бот, неправомерный вход в информационную систему или покупка готовой детализации имеют разное уголовно-правовое значение. Законный способ получения может исключать преступность, тогда как скрытый доступ к биллинговой системе или приобретение незаконной выгрузки требует проверки уголовных составов.

Третий критерий — лицо, имеющее доступ. Если сведения выгружает работник оператора связи, вопрос о служебном положении относится к нему. Если сведения передаёт посредник, необходимо установить его роль и источник доступа. Если частный детектив лишь получает результат, надо определить, знал ли он о незаконном происхождении сведений, организовывал ли получение, оплачивал ли доступ и передавал ли результат заказчику.

Четвёртый критерий — профессиональная связь с частной сыскной деятельностью. Договор, поручение, оплата, отчёт, переписка с заказчиком, передача результата и использование статуса частного детектива могут свидетельствовать о том, что деяние совершено не как бытовое информационное нарушение, а как часть детективной услуги. Именно этот элемент имеет значение для проверки ст. 203 УК РФ [11; 12; 13].

Пятый критерий — характер вреда. Сведения о соединениях могут нарушать тайну связи, а в сочетании с иными данными — частную жизнь. Если они хранятся и передаются в цифровой форме, возникает вопрос о компьютерной информации и персональных данных. Если сведения используются в конфликте, для давления, шантажа, имущественного или

⁸Савеловский районный суд г. Москвы. Приговор от 04.04.2019. Дело № 01-0138/2019.

⁹Ленинский районный суд г. Иваново. Приговор от 19.09.2025. Дело № 1-223/2025. Дикушин А.Ю.

семейного воздействия, это усиливает общественную опасность деяния.

Шестой критерий — наличие самостоятельных составов. Если нарушена тайна связи, проверяется ст. 138 УК РФ. Если данные получены через неправомерный доступ к системе, проверяется ст. 272 УК РФ. Если речь идёт о компьютерной информации, содержащей персональные данные, проверяется ст. 272.1 УК РФ. Если сведения раскрывают частную жизнь, возможна оценка по ст. 137 УК РФ. Если деяние совершено в профессиональном контексте частного сыска, дополнительно проверяется ст. 203 УК РФ.

Таким образом, уголовно-правовая оценка должна быть многоэлементной. Недостаточно установить, что частный детектив «получил детализацию». Нужно определить, какие сведения получены, как именно они добыты, кто имел доступ, кому они переданы, в каком конфликте использованы и связано ли получение с частной сыскной деятельностью.

Заключение.

Сведения о телефонных соединениях, базовых станциях и местоположении абонентского устройства не являются обычной справочной информацией. Они позволяют восстановить коммуникационные, социальные, семейные, деловые и пространственные связи лица, а потому находятся в зоне действия специальных правовых режимов: тайны связи, защиты частной жизни, персональных данных и охраняемой компьютерной информации.

Частный детектив не вправе получать такие сведения только на основании лицензии или поручения заказчика. Наведение справок в частной сыскной деятельности не включает доступ к биллинговым системам операторов связи, детализации соединений, данным базовых станций или геолокации абонентского устройства. Получение этих данных через инсайдера, посредника, цифровой сервис или неправомерный доступ к информационной системе должно оцениваться как возможное посягательство на самостоятельные уголовно охраняемые объекты.

Служебный доступ к сведениям о соединениях может иметь работник оператора связи или иной обладатель технического доступа, но не частный детектив по факту наличия лицензии. Поэтому при квалификации необходимо разграничивать действия инсайдера, посредника, частного детектива и заказчика. Если незаконное получение сведений связано с выполнением или имитацией детективного поручения, дополнительно проверяется наличие признаков ст. 203 УК РФ.

Уголовно-правовая оценка получения частным детективом сведений о соединениях и геолокации должна строиться через сочетание информационного режима сведений и профессионального контекста частного сыска: первое определяет применимость специальных информационных составов, второе — возможность дополнительной оценки по ст. 203 УК РФ.

Конфликт интересов

Не указан.

Conflict of Interest

None declared.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. Юрченко И.А. Нарушение телекоммуникационной тайны в контексте российского уголовного права: текущие проблемы и перспективы их преодоления // *Lex Russica*. 2023. Т. 76. № 9 (202). С. 44-58. DOI: 10.17803/1729-5920.2023.202.9.044-058 EDN: PKTERQ
2. Федотова Н.В. Уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений: дис. ... канд. юрид. наук. М., 2009. 171 с. EDN: QEGJRR
3. Жеребкин В.П. Уголовно-правовая охрана частной жизни: дис. ... канд. юрид. наук. Саратов, 2003. 197 с. EDN: NMOGNB
4. Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. М., 2003. 155 с. EDN: NODYZP
5. Песков П.Д., Помнина С.Н. Актуальные вопросы квалификации состава преступления, предусмотренного ст. 272 УК РФ // *Огарёв-online*. 2024. Т. 12. № 16. С. 46-53. DOI: 10.15507/ogarev-online.v12i16.278133.
6. Князьков А.А. Уголовно-правовая новелла за нарушение законодательства о персональных данных (ст. 272.1 УК РФ): особенности конструирования состава и вопросы квалификации // *Вестник Университета имени О.Е. Кутафина*. 2025. № 5 (129). С. 65-73. DOI: 10.17803/2311-5998.2025.129.5.065-073 EDN: CHMJWG
7. Петроченков С.Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации : дис. ... канд. юрид. наук. М., 2013. 174 с.
8. Артемов В.В. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, в уголовном праве России : дис. ... канд. юрид. наук. М., 2011. 206 с.
9. Борбат А.В. Квалификация преступления, предусмотренного ст. 203 УК РФ, по признакам субъективной стороны // *Российский следователь*. 2016. № 14. С. 11-13. DOI: 10.18572/1812-3783-2016-14-11-13 EDN: WICWHH
10. Федорова Е.Л. Превышение полномочий частным детективом или работником частной охранной организации, совершенное с использованием оружия или специальных средств и повлекшее тяжкие последствия: вопросы квалификации // *Сибирский юридический вестник*. 2024. № 1. С. 95-101. DOI: 10.26516/2071-8136.2024.1.95 EDN: WWAVSM
11. Овчаров А.В. Уголовная ответственность за превышение полномочий служащими частных охранных и детективных служб: дис. ... канд. юрид. наук. М., 2002. 186 с. EDN: NMCMAZ

12. Чурсина И.В. Уголовная ответственность за превышение полномочий частным детективом или работником частной охранной организации: автореф. дис. ... канд. юрид. наук. Хабаровск, 2016. 26 с. EDN: ZQCOYD
13. Волков К.А. Квалификация превышения полномочий частным детективом или работником частной охранной организации // *Законность*. 2016. № 4. С. 49-53. EDN: WCFZAP

References:

1. Yurchenko I.A. Violation of telecommunication secrecy in the context of Russian criminal law: current problems and prospects for overcoming them // *Lex Russica*. 2023. Vol. 76. No. 9 (202). pp. 44-58. DOI: 10.17803/1729-5920.2023.202.9.044-058 EDN: PKTERQ
2. Fedotova N.V. Criminal liability for violating the secrecy of correspondence, telephone conversations, postal, telegraphic and other communications: dis. ... kand. jurid. nauk. M., 2009. 171 p. EDN: QEGJRR
3. Zherebkin V.P. Criminal and legal protection of private life: dis. ... kand. jurid. sciences'. Saratov, 2003. 197 p. EDN: NMOGNB
4. Doronin A.M. Criminal liability for unlawful access to computer information: dis. ... kand. jurid. nauk. M., 2003. 155 p. EDN: NODYZP
5. Peskov P.D., Pomnina S.N. Actual issues of qualification of the corpus delicti provided for in art. 272 of the Criminal Code of the Russian Federation // *Ogarev-online*. 2024. Vol. 12. No. 16. pp. 46-53. DOI: 10.15507/ogarev-online.v12i16.278133.
6. Knyazkov A.A. Criminal law novella for violation of the legislation on personal data (art. 272.1 of the Criminal Code of the Russian Federation): design features of the composition and qualification issues // *Bulletin of the O.E. Kutafin University*. 2025. No. 5 (129). pp. 65-73. DOI: 10.17803/2311-5998.2025.129.5.065-073 EDN: CHMJWG
7. Petrochenkov S.D. Criminal liability for the illegal trafficking of special technical means intended for the secret receipt of information : dis. ... kand. jurid. nauk. M., 2013. 174 p.
8. Artyomov V.V. Illegal receipt and disclosure of information constituting a commercial, tax or banking secret in the criminal law of Russia : dis. ... kand. jurid. Nauk. M., 2011. 206 p
9. Borbat A.V. Qualification of the crime under Article. 203 of the Criminal Code of the Russian Federation on the grounds of the subjective side // *Russian investigator*. 2016. No. 14. PP. 11-13. DOI: 10.18572/1812-3783-2016-14-11-13 EDN: WICWHD
10. Fedorova E.L. Abuse of authority by a private detective or an employee of a private security organization, committed using weapons or special means and entailing grave consequences: qualification issues // *Siberian Law Bulletin*. 2024. No. 1. pp. 95-101. DOI: 10.26516/2071-8136.2024.1.95 EDN: WWAVSM
11. Ovcharov A.V. Criminal liability for abuse of authority by employees of private security and detective services: dis. ... kand. jurid. nauk. M., 2002. 186 p. EDN: NMCMAZ
12. Chursina I.V. Criminal liability for abuse of authority by a private detective or an employee of a private security organization: abstract of the dissertation. ... kand. jurid. sciences'. Khabarovsk, 2016. 26 p. EDN: ZQCOYD
13. Volkov K.A. Qualification of abuse of authority by a private detective or an employee of a private security organization // *Legality*. 2016. No. 4. pp. 49-53. EDN: WCFZAP

Информация об авторе:

Швецов Роман Евгеньевич, адвокат Адвокатской палаты города Москвы; соискатель ученой степени кандидата юридических наук Российского университета адвокатуры и нотариата имени Г. Б. Мирзоева, кафедра адвокатуры и уголовно-правовых дисциплин имени А. В. Клигмана; e-mail: 615007@gmail.com. ORCID: 0009-0002-1111-0240

Roman E. Shvetsov, Advocate of the Moscow Chamber of Advocates; applicant for the academic degree of Candidate of Legal Sciences, G. B. Mirzoev Russian University of Advocacy and Notariat, A. V. Kligman Department of Advocacy and Criminal Law Disciplines.

Статья поступила в редакцию / The article was submitted 17.02.2026;
Одобрена после рецензирования / Approved after reviewing 06.07.2026;
Принята к публикации / Accepted for publication 20.09.2026.
Автором окончательный вариант рукописи одобрен.