Жандров В. Ю.[1],
доцент кафедры оперативно-разыскной деятельности
и специальной техники
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ЭЛЕКТРОННОЕ НАБЛЮДЕНИЕ В МЕХАНИЗМЕ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ

Развитие информационно-телекоммуникационных технологий (далее – ИТК) повлекло расширение возможностей их использования криминалитетом для повышения анонимности коммуникации и дистанционного совершения преступлений. Примечательно, что именно наркоторговля стала пионером использования инновационных IT-решений, которые начали апробироваться вовлеченными лицами уже в 2000 гг. В сфере незаконного оборота наркотиков (НОН) произошла трансформация способов сбыта запрещенных веществ, вследствие которой в их структуре стало преобладать бесконтактное проведение преступных сделок. Новый способ сбыта наркотиков исключил прямое физическое взаимодействие между покупателями и продавцами, поскольку оказался способен опираться на анонимные каналы связи, поддерживаемые новыми платформами обмена сообщениями, а также на использование цифровых валют для осуществления транзакций.

На фоне произошедших изменений практика документирования преступной деятельности фигурантов сформировала очевидный запрос на поиск новой тактики проведения оперативно-разыскных[2] мероприятий (ОРМ), методы которой соответствовали бы новым криминальным реалиям. Закономерным шагом на пути поиска новых подходов выявления и документирования НОН стало обращение внимания теории оперативно-разыскной деятельности (ОРД) к такому специальному методу расследования как электронное наблюдение.

Появление термина «электронное наблюдение» связывают с периодом действия «сухого закона» в США (1920−1930-е гг.), когда впервые в правоприменительной практике для борьбы с подпольным производством и торговлей алкоголем было использовано мероприятие «подслушивание телефонных переговоров» [7]. С течением времени появление разнообразных способов передачи информации сопровождало использование и новых негласных способов ее перехвата – «слухового контроля переговоров» и «видеоконтроля помещений и местности», которые также рассматривались в качестве способов электронного наблюдения.

Нормативное закрепление термина «электронное наблюдение» связывают с принятием Закона США 1978 г. «О контроле за внешней разведкой» [3],

---

[1] © Жандров В. Ю., 2024.

[2] Здесь и далее написание слова *разыскной* приводится в соответствии с нормами русского языка, за исключением употребления в нормативных правовых актах.

и последующим его распространением на расследование обычных преступлений Законом США 1986 г. «О конфиденциальности электронных коммуникаций (ECP) [4].

В международном праве термин «электронное наблюдение» впервые был использован ст. 20 Конвенции ООН против транснациональной организованной преступности (принята Резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 г.) [1], а затем воспринят и ст. 50 Конвенции ООН против коррупции (принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003) [2]. В обоих документах электронное наблюдение определено в качестве специального метода расследования по уголовным делам.

Именно в таком значении электронное наблюдение нашло свое отражение в акутализированном Управлением ООН по наркотикам и преступности в 2022 г. Модельном законе о взаимной правовой помощи по уголовным делам 2007 г. (в ред. 2022 г.) при формулировании положений об электронных доказательствах [5]. Определение упомянутого закона раскрывает «электронное наблюдение» через два вида мониторинга [6]:

– мониторинг, перехват, копирование или манипулирование сообщениями, данными или сигналами, которые хранятся, передаются или находятся в процессе передачи электронными средствами;

– мониторинг или запись деятельности с помощью электронных средств, а также любое скрытое участие в электронной связи с подозреваемыми, связанная с проведением агентурных мероприятий.

Обращение к международному опыту, практике законодательного регулирования зарубежных стран, а также возможностям современных информационно-телекоммуникационных технологий полагаем возможным в самом первом приближении очертить рамки электронного наблюдениями следующими мерами:

– электронный мониторинг местоположения мобильного объекта;

– прослушивание телефонных переговоров;

– перехват актов коммуникации и мониторинг преступной активности в режиме online посредством удаленной активации камер и микрофонов электронных мобильных устройств;

– мониторинг социальных сетей, получение доступа к аккаунтам, подключение к наркориентированным онлайн-сообществам;

– получение и анализ данных из открытых электронных источников;

– получение контроля над ЭМУ для ознакомления с текстами сообщений и внутренней информацией устройства;

– зашифрованное участие в электронном общении с подозреваемым в совершении преступления с целью сбора доказательств или проверки оперативной информации.

Некоторые из перечисленным мер очевидно перекрываются положениями Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», который в ст. 6 закрепляет прослушивание телефонных переговоров, снятие информации с технических каналов связи и получение компьютерной информации в числе ОРМ. Безусловно, возможно расширительно трактовать

содержание регулируемых законом мероприятий, однако в реалиях неоднозначности соблюдения конституционных прав человека в цифровой среде этот подход может оказаться не вполне удачным и привести к их нарушению в рамках ОРД.

Различие между традиционным сбором цифровых данных в ходе уголовного судопроизводства и получением доказательств в Интернет заключается в методах и инструментах, используемых для проверки и аутентификации, в соответствии с требованием действующего законодательства. При этом простого создания снимков экрана или использования изображений с цифровой камер уже недостаточно для документирования преступлений в информационно-телекоммуникационной среде. В связи с чем встает проблема аутентификации (англ. *authentication* – «реальный, подлинный» – процедура проверки подлинности), которую необходимо решить в ходе проведения оперативно-розыскных мероприятий, чтобы обеспечить допустимость информации, хранящейся в электронном виде, для целей уголовного судопроизводства. Конечной точкой здесь будет являться надлежащее получение и процессуальное закрепление интернет-данных, выраженных в цифровой форме, хранящиеся на каком-то устройстве.

Вышеизложенное позволяет сформулировать ряд положений, имеющих значение для совершенствования механизма выявления и документирования незаконного оборота наркотиков:

1. В условиях цифровизации и стремительного развития ИТК неминуемой становится трансформация ОРД по противодействию НОН, осуществляемому бесконтактным способом. Данный процесс должен сопровождаться пересмотром тактики проведения ОРМ за счет расширения приемов и способов сбора электронных доказательств.

Поскольку действующее оперативно-розыскное законодательство не охватывают всех тех возможностей, которые предоставляют современные ИТК, постольку совершенствования механизма выявления и документирования НОН в современных условиях возможно достичь за счет развития теоретических и законодательных положений об электронном наблюдении как относительно самостоятельном методе ОРД, включающем перечень специальных мер по слежению, контролю и фиксации действий фигурантов с помощью современных ИТК.

2. Включение электронного наблюдения в российскую практику ОРД по противодействию НОН отвечает как новым вызовам в этой сфере, так и современной конфигурации правового обеспечения этой деятельности. Во-первых, расширение перечня специальных методов расследования за счет включения мероприятий, имеющих специфические функции, отражает объективно сложившуюся потребность правоохранительных органов в фиксации картины произошедших преступных событий в Интернет и смежной с ней цифровой среде. Во-вторых, Российская Федерация является участником ряда международных конвенций, предусматривающих электронное наблюдение в качестве специального метода расследования, в связи с чем в соответствии с принципами отечественной правовой системы и в пределах своих возможностей принимает необходимые меры для реализации положений ратифицированных документов, направленных на обеспечение надлежащего процесса сбора доказательств, в том числе электронных.

Список литературы

1. Конвенция Организации Объединенных Наций против транснациональной организованной преступности : принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 г. URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml.

2. Конвенция Организации Объединенных Наций против коррупции : принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003 г. URL: https://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml.

3. 50 Кодекс США, глава 36 «Надзор внешней разведки». URL: https://www.law.cornell.edu/uscode/text/50/chapter-36.

4. Electronic Communications Privacy Act of 1986 (ECPA). URL: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

5. Model Law on Mutual Assistance in Criminal Matters. URL: https://sherloc.unodc.org/cld/uploads/pdf/El%20Evidence%20Hub/Model_Law_on_MLA_2007.pdf.

6. Типовой закон о взаимной помощи по уголовным делам (2007 г.), с поправками, включающими положения об электронных доказательствах и применение специальных методов расследования (2022 г.) (п. 7 р. 27 ч. 4). URL: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_31/CRP/E_CN15_2022_CRP6_e_V2202980.pdf.

7. Самохин Б. М., Князев В. В. Зарубежный опыт оперативно-розыскной деятельности в борьбе с преступностью : научный обзор. М.: ВНИИ МВД СССР, 1991.