Об отражении в оперативно-розыскном законодательстве вопросов использования больших данных в оперативно-розыскной деятельности

А. Л. Осипенко –

заместитель начальника Воронежского института МВД России по научной работе, доктор юридических наук, доцент

Совершенствование оперативно-розыскного законодательства в современных условиях невозможно без учета социальных и технологических процессов, оказывающих существенное влияние на изменение характера оперативно-розыскной деятельности и в первую очередь на способы добывания оперативно значимой информации. Причем если еще совсем недавно основным вектором интенсификации получения такой информации можно было считать повышение эффективности использования ресурсов сети Интернет, то сегодня этот вектор меняет направление в сторону обработки так называемых больших данных.

Важно видеть, что в последние годы спектр технических источников оперативно-розыскных данных постоянно расширяется. Выделим лишь основные направления внедрения новых технологий, оказывающих влияние на изменение закономерностей образования и концентрации оперативно значимой информации:

– развитие информационных ресурсов сети Интернет и предлагаемых в ней сервисов, сопровождаемое нарастанием интенсивности сетевых взаимодействий между гражданами и социальными структурами;

– беспрецедентный охват населения средствами сотовой связи и мобильными устройствами, обеспечивающими доступ к сетевым ресурсам;

– расширение применения систем геопозиционирования, позволяющих осуществлять привязку различных физических объектов к их положению на местности;

– увеличение мощности вычислительных систем, обеспечившее условия для широкого внедрения технологий распознавания образов (лица, голос, номерные знаки автотранспортных средств и др.), и наращивание арсенала использующих эти технологии систем видеонаблюдения и видеорегистраторов;

– осуществление видеомониторинга территорий и объектов с использованием беспилотных летательных аппаратов;

– расширение применения разного рода нательных датчиков (например, фиксирующих физиологические показатели или принудительно закрепляемых для ограничения свободы передвижения);

– резкий рост видов, количества и функций так называемых умных вещей, оснащенных микропроцессорами и способных осуществлять обмен данными с телекоммуникационными сетями (системы умного дома, бытовые приборы, оргтехника, навигационные системы автотранспорта, информационные датчики в местах общественного пользования и т. п.);

– развитие технологий дополненной реальности, обеспечивающих непрерывный доступ индивидуума к мобильной телекоммуникационной среде и постоянное поступление информации, влияющей на принятие им решений.

Если все описанное многообразие устройств и систем рассматривать с позиций решения задач оперативно-розыскной деятельности, то источниками оперативно значимой информации можно считать различные информационные системы государственных органов и коммерческих структур, в том числе операторов связи, потоки данных от различных датчиков (радиочастотных идентификаторов, GPS-трекеров и т. п.), стационарных и мобильных измерительных устройств, систем геопозиционирования, видеонаблюдения и видеофиксации, сообщения из

социальных сетей и иных мест сетевого общения объектов оперативного интереса. Благодаря постоянному снижению стоимости хранения информации в электронной форме поступающие из этих источников огромные массивы цифровых данных могут быть сохранены и использованы для автоматизированной обработки. Однако анализ таких неструктурированных данных, поступающих из разных источников, во всей их полноте с извлечением нового знания продолжает оставаться сложной задачей. Для ее решения формируются новые концептуальные подходы, объединяемые понятием «большие данные».

Термин «большие данные» появился относительно недавно, но довольно быстро закрепился в научной и деловой литературе, и сегодня его широко используют крупнейшие разработчики программно-аппаратных средств обработки информации и ведущие аналитики рынка информационных технологий. Под большими данными понимают колоссальные по объемам структурированные и слабоструктурированные массивы данных, представленных в самых разнообразных форматах и хранящихся распределенно в различных узлах глобальной Сети. Следует учитывать, что происходит постоянное пополнение этих массивов при увеличении их числа, обеспечивающее высочайшие скорости прироста совокупных данных.

Обработка таких данных с комплексным использованием особых подходов, специальных инструментов и методов (например, методов массово-параллельной обработки) позволяет получать в различных сферах деятельности (производстве, здравоохранении, торговле, государственном управлении) новые ценные знания, недостижимые иными способами. Важно, что анализ больших данных способен обеспечить преимущество во всех сферах деятельности, связанных с интеллектуальным противоборством и необходимостью получения разведывательной информации. Это, разумеется, относится и к оперативно-розыскной деятельности, где происходит

интеллектуальное противостояние правоохранительных органов с организованной преступностью.

В настоящее время ряд корпораций (IBM, Oracle, Teradata, EMC и др.) предлагают готовые программные решения и аппаратно-программные комплексы для массово-параллельной обработки данных, позволяющие агрегировать данные объемом в десятки терабайт и производить их глубокий анализ, обеспечивающие обнаружение неизвестных событий, автоматизированное выявление латентных связей между объектами различной природы (событиями, людьми, предметами, сведениями и др.), визуализацию результатов о наличии неявных связей, структуру которых трудно передать иными способами. Известно, что анализ больших данных уже активно проводится спецслужбами США, других государств. Управление перспективных исследований при Министерстве обороны США (DARPA) запустило программу MEMEX, с помощью которой анализирует скрытые зоны Интернета, чтобы контролировать, как в них общаются участники международных преступных сетей. Есть свидетельства того, что в США ведется активная разработка и практическое использование технологий управления групповым и массовым поведением граждан в других странах мира[1].

Очевидно, что анализ больших данных позволит решать широкий спектр важных оперативно-розыскных задач:

– обеспечивать сбор максимально полной информации об объектах оперативного интереса с формированием электронного досье на потенциальных преступников, обнаружением и визуализацией неявных связей с иными объектами и событиями криминального характера;

– фиксировать социальную активность разрабатываемых лиц, возникновение и изменение их сетевых связей, анализировать степень

[1] См.: *Овчинский В. С., Ларина Е.* Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М., 2014. С. 50.

интереса к тем или иным обсуждаемым в местах сетевого общения событиям;

– отслеживать появление в киберпространстве цифровых следов с заданными свойствами, указывающими на высокую вероятность подготовки либо совершения криминальных действий, и оповещать оперативных сотрудников;

– строить и проверять в автоматизированном режиме оперативно-розыскные версии;

– выявлять группировки криминальной направленности (в том числе имеющие сетевую форму организации с гибкой структурой), определять их специализацию, степень организованности, распределение ролей, характер неочевидных связей между фигурантами и их причастность к тем или иным событиям;

– строить поведенческие профили для лиц, совершающих преступления определенных видов, и формировать на этой основе поведенческие гипотезы;

– улучшать планирование оперативно-розыскных действий за счет учета сложной совокупности многочисленных факторов, влияющих на развитие конкретной оперативно-тактической ситуации.

Наконец, что очень важно, анализ больших данных создает реальную технологическую основу использования оперативно-розыскных методов для прогнозирования различных социально опасных событий и предупреждения преступлений. Исследователи отмечают, что системы на основе больших данных «направлены на профилактику преступлений путем их прогнозирования вплоть до выявления частных лиц, которые могут их совершить»[2].

Безусловно, специфика больших данных не может не отражаться на правовом регулировании применения оперативно-розыскных методов при их

[2] См.: *Майер-Шенбергер В., Кукьер К.* Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. М., 2014.С. 51.

получении и обработке. Здесь остро стоит целый ряд вопросов, связанных в первую очередь с обеспечением прав граждан; определением пределов полномочий оперативно-розыскных органов в наднациональном сетевом пространстве; регламентацией взаимодействия операторов связи, провайдеров интернет-ресурсов, владельцев информационных систем с органами, осуществляющими ОРД.

Особый блок составляют проблемы соблюдения прав граждан при обработке оперативно-розыскными органами данных, отражающих обстоятельства их частной жизни. Не вызывает сомнений, что с развитием технологий сбора больших данных из всех возможных источников эти проблемы будут только усугубляться. Попадая в Интернет, сведения о частной жизни лица выходят из-под контроля субъекта распространения, могут массово дублироваться на многочисленных информационных ресурсах и храниться там неограниченно долго. Нередко возникают ситуации, когда пользователь не в состоянии удалить из сети информацию о себе. Известно решение Европейского Суда по правам человека, по которому гражданин ЕС вправе требовать от владельцев поисковых систем исключать из результатов поиска ссылки на документы, содержащие сведения о нем, не соответствующие действительности. Европейский Суд назвал это «правом на забвение». В нашей стране Общественная палата рекомендовала подготовить законопроект, обеспечивающий аналогичную защиту персональных данных для российских пользователей Интернета. Между тем, на наш взгляд, реализация такого права на практике будет крайне затруднительной, если не сказать невозможной.

Важно учитывать, что в условиях повышенной информационной прозрачности, создаваемой постоянным накоплением и неконтролируемым дублированием в Интернете информации о гражданах, практически нереально обеспечить полное сохранение тайны их частной жизни. Большинство из нас, не задумываясь об этом, постоянно оставляет цифровые следы своей сетевой активности. При этом все больше размывается грань

между конфиденциальными и общедоступными данными, которые без ограничений могут обрабатываться как большие данные.

Тем не менее думаем, что полномочия полиции по мониторингу персональных данных граждан, контролю за электронной перепиской разрабатываемых лиц, автоматизированному сбору и анализу разрозненных сведений об их поведении, связях, интересах, финансовых операциях, местонахождении и перемещениях, формированию «электронного досье» должны быть четко регламентированы в соответствующих нормативных правовых актах.

Естественно, расширение возможных форм электронного контроля за гражданами и отслеживания их социальной активности со стороны правоохранительных органов резко обостряет задачу поиска оптимального соотношения между интересами личности и общества. Отметим, что в последнее время во многих государствах проявляется тенденция изменения баланса приоритетов в пользу защиты общественных, государственных интересов. К сожалению, попытки устранить определенные пробелы в отечественном законодательстве, регулирующем правовые отношения в сфере информационных технологий, пока не имеют продуманного концептуального подхода. В таких условиях вопросы обеспечения прав граждан при осуществлении оперативно-розыскной деятельности с использованием информационно-телекоммуникационных технологий должны привлекать повышенное внимание ученых и находить соответствующую теоретическую проработку.

Особую важность приобретает создание реальных правовых условий для концентрации и обработки больших данных. Для этого должна быть сформирована продуманная правовая основа передачи в распоряжение оперативно-розыскных органов максимального количества рассмотренных ранее информационных массивов.

Так, в заметной степени права граждан ограничиваются при проведении оперативно-розыскных мероприятий, направленных на сбор

информации, содержащей их персональные данные. В то же время использование оперативными подразделениями технологий больших данных невозможно без получения максимального доступа к информационным системам государственных органов и коммерческих структур, операторов связи, провайдеров интернет-ресурсов, системам геопозиционирования, видеонаблюдения и видеофиксации. Владельцы указанных систем в соответствии с законодательством обязаны обеспечивать защиту персональных данных граждан, сведения о которых обрабатываются в них. Напротив, обязанность и условия предоставления доступа к обрабатываемым в названных системах данным субъектам ОРД при решении ими задач оперативно-розыскной деятельности в федеральных законах не обозначены. Вернее, это сделано лишь по отношению к операторам связи (провайдерам сети Интернет) при исполнении закрепленной Федеральным законом «О связи» обязанности предоставлять субъектам ОРД информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения задач, возложенных на оперативно-розыскные органы. Полагаем, аналогичные обязанности и условия их реализации должны быть закреплены для владельцев всех информационных систем, данные из которых могут быть эффективно использованы в оперативно-розыскной деятельности. Стоит добавить, что подобные правовые нормы имеются в законодательстве США.

Особого исследования заслуживает вопрос правового регулирования использования в интересах оперативно-розыскной деятельности массивов персональных данных при условии, что оператор их обработки передает такие массивы субъекту ОРД, предварительно их обезличив (например, заменив конкретные имена последовательностью номеров). Очевидно, что предоставление массивов обезличенных данных для обработки не ограничивает конституционные права граждан и, соответственно, может производиться без судебного решения. Действительно, в определенных ситуациях субъекту ОРД достаточно лишь проверить версию о том,

действительно ли имело место сочетание каких-либо событий (например, серия звонков на заданный номер с одного и того же абонентского номера и посещение определенного объекта владельцем этого номера в заданном временном промежутке). При подтверждении такой версии для обезличенного абонента его персональные данные могут быть получены уже в установленном законом порядке после получения судебного решения.

Наконец, при обработке больших данных, значительная часть из которых циркулирует в наднациональном киберпространстве сети Интернет, могут возникать ситуации столкновения различных интересов и правовых систем. Такое положение дел требует соответствующей регламентации в международных актах. Стоит отметить, что согласование международных правовых средств в изучаемой сфере затрудняется не только существенными различиями в правовых системах государств, но и спецификой объекта правового регулирования. Одной из проблем, становящейся здесь основным камнем преткновения, является проблема определения юрисдикции государства в киберпространстве. Для ОРД актуальность данной проблемы состоит в первую очередь в том, что от вариантов ее решения напрямую зависят пределы полномочий национальных оперативно-розыскных органов, а следовательно, и допустимость осуществления ими отдельных трансграничных действий в киберпространстве с учетом наднациональной природы последнего. На наш взгляд, есть необходимость в дополнении рассматриваемого проекта Оперативно-разыскного кодекса статьей, определяющей особенности проведения оперативно-розыскных мероприятий с использованием информационно-телекоммуникационных сетей международного информационного обмена.

Подводя итог, стоит подчеркнуть, что организованная преступность также проявляет интерес к технологиям больших данных, а отставание оперативных подразделений в овладении ими крайне опасно. Поэтому особую важность приобретает скорейшее внедрение названных технологий в оперативно-розыскную деятельность. Разумеется, для того чтобы обеспечить

эффективное использование больших данных в оперативно-розыскной деятельности, необходимо не только создать очень дорогостоящую технологическую основу и решить сложные вопросы кадрового обеспечения, но и тщательно проработать соответствующие правовые нормы, ясно и четко регулирующие вопросы, связанные с порядком доступа к большим данным, их обработки и использования ее результатов.

Для оформления ссылки на данную публикацию:

Осипенко А.Л. Об отражении в оперативно-розыскном законодательстве вопросов использования больших данных в оперативно-розыскной деятельности // Актуальные вопросы законодательного регулирования оперативно-разыскной деятельности: материалы всероссийской научно-практической конференции. Омская юридическая академия. 2015. С. 46-53.