

А. Н. Лахин

СОВЕРШЕНСТВОВАНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ ТЕХНОЛОГИЙ ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Мировой научно-технический прогресс привел к массовому использованию населением электронных устройств и накоплению колоссального объема сведений, хранящихся в различного рода цифровых, в том числе автоматизированных (автоматических), банках данных.

Для оперативных подразделений правоохранительных органов особую актуальность приобретает вопрос о правовом регулировании получения накапливаемых данных в свое распоряжение для проведения анализа и использования их в целях выявления и раскрытия совершенных преступлений. Сегодня существует очевидный законодательный перекося: одни структуры получают беспрепятственный доступ к таким сведениям (например, к информации по операциям, счетам и вкладам физических лиц, которая выдается руководителям и должностным лицам федеральных государственных органов без судебного решения), а оперативным подразделениям для аналогичного доступа требуется разрешение судебных органов.

Соответственно, действующее законодательство в области использования новейших технологий получения и обработки информации (информационно-аналитических технологий) оперативно-разыскными органами нуждается в совершенствовании и доработке. Вслед за изменениями, происходящими в обществе, связанными с развитием информационно-аналитических и телекоммуникационных технологий, постоянного реформирования требует нормативно-правовая база, регулирующая отношения, которые возникают при их использовании в оперативно-разыскной деятельности.

Ключевые слова: информационно-аналитические технологии, оперативные подразделения, оперативно-разыскная деятельность, доступ, правовое регулирование.

A. N. Lakhin

LEGAL REGULATION OF USE OF INFORMATION TECHNOLOGIES BY OPERATIONAL DIVISIONS OF LAW-ENFORCEMENT BODIES

World scientific and technical progress led to wide circulation of various electronic devices among the population, and also to accumulating of enormous amount of the data which are stored in different digital, including automated (automatic) databanks.

For operational divisions of law enforcement agencies urgent is a question of legal regulation of receipt of the accumulated data in the order for carrying out the analysis and their use for the purpose of identification and disclosure of the committed crimes. There is an obvious legislative distortion allowing one structures easy access to such data today (for example, to information on transactions, accounts and household deposits which is issued to heads and officials of federal state bodies without judgment). Whereas operational divisions for similar access need permission of judicial authorities.

Respectively, the current legislation in the field of use of the latest technologies of obtaining and information (information and analytical) processing by operational search bodies needs enhancement and completion. After the changes happening in society, connected with development of information and analytical and telecommunications technologies the regulatory framework governing the relations which arise in case of their use in operational search activities requires fixed reforming.

Key words: information and analytical technologies, operational divisions, operational search activities, access, legal regulation.

Современный высокий уровень развития информационных, информационно-аналитических и телекоммуникационных технологий, стремительная интенсификация их использования физическими и юридическими лицами, а также органами

государственной власти были спрогнозированы еще в 2008 г. в Стратегии развития информационного общества в Российской Федерации [1].

Мировой научно-технический прогресс привел к тому, что сегодня население полностью

обеспечено средствами сотовой связи и мобильными устройствами. Широкое распространение получили системы геопозиционирования и распознавания образов (лица, голоса, номерных знаков автотранспортных средств и др.), видеонаблюдения и видеорегистрации. Различные организации используют видеомониторинг территорий и объектов, осуществляемый с помощью беспилотных летательных аппаратов, применяют разного рода датчики (например, фиксирующие физиологические показатели или принудительно закрепляемые для ограничения свободы передвижения отдельных лиц). Одновременно в обороте у населения растет число устройств (очки Google), облегчающих ориентацию в незнакомом месте, поиск объектов с заданными свойствами, распознавание зданий и сооружений, получение в режиме реального времени данных о технических характеристиках конкретных устройств и др. [2].

Более того, увеличивается количество видов 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.) [2].

Перечисленные обстоятельства порождают накопление колоссального объема сведений, хранящихся в различного рода цифровых, в том числе автоматизированных (автоматических), банках данных. При этом отдельную категорию составляют массивы оцифрованных данных, образующихся в ходе деятельности юридических лиц, государственных органов власти и управления, а также органов местного самоуправления.

С учетом внедрения информационных, информационно-аналитических и телекоммуникационных технологий во все сферы нашей жизни, а также постепенного перехода документооборота всех, в том числе государственных, организаций в электронную форму для правоохранительных органов и в первую очередь их оперативных подразделений особую актуальность приобретает вопрос о правовом регулировании оперативного получения этих накапливаемых данных в свое распоряжение для проведения анализа и использования в решении стоящих перед ними задач*. Однако этот процесс сопровождается трудностями. Причин для этого несколько. Для получения и анализа оперативно значимых сведений, вычленения их из всего объема доступных данных сотрудникам оперативных

подразделений необходимо использовать постоянно обновляющиеся высокопроизводительные информационно-аналитические технологии добытия и обработки информации [3]. Вместе с тем их применение должно получить четкую регламентацию (законодательное урегулирование), что позволит безоговорочно использовать получаемые знания при принятии решений в рамках уголовного судопроизводства. Очевидно, что сформировать универсальное законодательство, которое одинаково эффективно регулировало бы возникающие правоотношения при изменении и появлении новых средств, методов и способов, применяемых в работе правоохранительных органов, сложно. В связи с этим реформирование нормативно-правовой базы должно быть постоянным, учитывать стремительно меняющуюся жизнь общества [4].

Конечно, передовые технологии получения и анализа информации используются всеми подразделениями правоохранительных органов [5]. Более того, о необходимости расширения их применения неизменно говорится на самом высоком уровне, в том числе в выступлениях Президента Российской Федерации В. В. Путина [6] и Министра внутренних дел Российской Федерации В. А. Колокольцева [7]. Но, на наш взгляд, наиболее приоритетной здесь все же является деятельность оперативных подразделений правоохранительных органов, поскольку именно от них зависят выявление и раскрытие совершенных преступлений.

Для того чтобы более точно понять круг законодательных проблем доступа к электронной информации, которые возникают в деятельности оперативных подразделений правоохранительных органов, необходимо провести разграничение между ними и подразделениями правоохранительных органов, не относящихся к числу оперативных.

Неоперативные подразделения применяют в своей деятельности информационно-аналитические технологии открыто (гласно) и по большей части работают с официальными данными. Получение следственными, экспертно-криминалистическими и другими неоперативными подразделениями официальных, в том числе используемых на предварительном следствии и в уголовном судопроизводстве, сведений, по нашему мнению, на законодательном уровне урегулировано в полной мере.

Оперативные подразделения, напротив, большую часть информации получают при проведении негласных мероприятий, соответственно, пользуются помимо официальных сведений оперативной информацией. Вместе с тем законодательные нормы, которые регулируют

применение информационно-аналитических технологий оперативными подразделениями, не охватывают весь круг возникающих отношений [3, 8]. Исходя из этого попробуем обозначить некоторые наиболее существенные проблемы правового регулирования применения информационно-аналитических технологий оперативными подразделениями органов внутренних дел. Для этого выделим основные вопросы, на которые в действующей нормативно-правовой базе пока нет однозначных ответов:

— обеспечение оперативного доступа к различным источникам информации;

— регламентация процедур получения оперативно значимой информации из многочисленных информационных систем;

— закрепление полномочий полиции по мониторингу персональных данных граждан;

— предоставление возможности контроля электронной переписки лиц, в отношении которых имеются сведения об их преступной деятельности, автоматизированного сбора и анализа разрозненных сведений об их поведении, связях, интересах, финансовых операциях, местонахождении и перемещениях, формирования «электронного досье»;

— установление пределов полномочий оперативных сотрудников по добыванию информации;

— обеспечение максимального доступа к информационным системам государственных органов и коммерческих структур, операторов связи, провайдеров интернет-ресурсов, системам геопозиционирования, видеонаблюдения и видеофиксации [3, 8].

В 2015 г. А. Л. Осипенко в работе «Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения» обосновал необходимость сбалансированного развития правовой основы использования информационно-аналитических технологий оперативными подразделениями органов внутренних дел, указав, что «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» [2].

На основе этого к ранее указанным вопросам правового регулирования, требующим своего решения, необходимо добавить следующие:

— обеспечение прав граждан при обработке оперативно-розыскными подразделениями персональных данных, а также при обработке сведений, отражающих обстоятельства их частной жизни;

— определение пределов полномочий оперативно-розыскных подразделений в наднациональном сетевом пространстве.

В списке нормативных актов, прямо регулирующих отношения, которые складываются при осуществлении оперативно-розыскной деятельности, первым следует назвать Федеральный закон «Об оперативно-розыскной деятельности» (далее — ФЗ «Об ОРД») от 12 августа 1995 г. № 144-ФЗ. Он определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Российской Федерации, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий [9].

В соответствии с ч. 3 ст. 4 ФЗ «Об ОРД» организация и тактика проведения оперативно-розыскных мероприятий с использованием специальных технических средств определяются ведомственными нормативными правовыми актами. Часть 1 ст. 12 этого же закона устанавливает, что сведения об используемых или использованных при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности, а также об организации и тактике проведения оперативно-розыскных мероприятий составляют государственную тайну.

На примере нескольких федеральных законов попробуем проанализировать ту нормативно-правовую базу оперативно-розыскной деятельности и использования информационно-аналитических технологий, которая находится в открытом доступе.

Как мы выяснили, ФЗ «Об ОРД» применительно к использованию информационно-аналитических технологий оперативными подразделениями не содержит норм, прямо их регулирующих. Однако косвенно такие нормы все же присутствуют.

Так, в части 3 ст. 6 сказано, что «в ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде». Другими словами, запрета на использование информационно-аналитических технологий нет, а под «техническими и иными средствами» можно понимать и аппаратно-программные комплексы, являющиеся составной частью информационно-аналитических технологий. В связи с этим можно сделать вывод о том, что использование информационно-аналитических технологий в оперативно-розыскной деятельности законодательно урегулировано и, соответственно, носит законный характер.

Вместе с тем ч. 1 ст. 10 ФЗ «Об ОРД» утверждает, что «органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них настоящим Федеральным законом, могут создавать и использовать информационные системы, а также заводить дела оперативного учета». По нашему мнению, данная норма не в полной мере отражает складывающуюся обстановку в сфере использования различного рода современных технологий. Содержащийся в ней термин «информационные системы» не охватывает понятие «информационно-аналитические технологии». Следовательно, в указанной статье отсутствует такая важная составляющая информационного обеспечения, как информационно-аналитические технологии. Для устранения этого пробела необходимо в ч. 1 ст. 10 ФЗ «Об ОРД» добавить слова «информационно-аналитические технологии», изложив ее в следующей редакции: «Органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них настоящим Федеральным законом, могут заводить дела оперативного учета, создавать и использовать информационные системы, а также использовать другие информационные и информационно-аналитические технологии».

Нормы, касающиеся соблюдения конституционных прав человека, закреплены в ч. 1 ст. 5 ФЗ «Об ОРД»: «Органы (должностные лица), осуществляющие оперативно-розыскную деятельность, при проведении оперативно-розыскных мероприятий должны обеспечивать соблюдение прав человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну корреспонденции». Законодатель четко урегулировал ограничения этих прав.

В соответствии с ч. 2 ст. 8 ФЗ «Об ОРД»: «Проведение оперативно-розыскных мероприятий (включая получение компьютерной информации), которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения». Таким образом, ФЗ «Об ОРД» допускает ограничение конституционных прав граждан, но только при получении соответствующего судебного решения. Вследствие этого данная норма сильно ограничивает использование информационно-аналитических технологий в оперативно-розыскной деятельности.

Вместе с тем в ч. 4 ст. 6 ФЗ «Об ОРД» определены субъекты, имеющие право проводить

мероприятия, ограничивающие конституционные права граждан, а также уточнен перечень проводимых ими мероприятий: «Оперативно-розыскные мероприятия, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов федеральной службы безопасности, органов внутренних дел».

В соответствии с перечнем оперативных подразделений системы МВД России, правомочных осуществлять оперативно-розыскную деятельность, к оперативно-техническим силам относятся подразделения специальных технических мероприятий (оперативно-технические подразделения) [10]. Следовательно, при возникновении необходимости получения информации с ограничением конституционных прав граждан сотрудникам оперативных подразделений системы МВД России необходимо обращаться в подразделения специальных технических мероприятий. Проведение таких мероприятий самостоятельно законом запрещено.

Ключевым моментом, разделяющим полномочия оперативно-технических и всех остальных оперативных подразделений системы МВД России, является необходимость получения информации с ограничением конституционных прав граждан, для которой нужно судебное решение. С учетом этого принципиально важно четко различать, что относится к информации, для получения которой необходимо судебное решение, а что к информации, для которой такое решение получать не надо.

В своей работе Б. П. Смагоринский, В. Б. Вехов и А. Н. Мартынов совершенно справедливо определяют круг информации, получаемой по судебному решению: «Любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью аппаратуры оператора связи, в том числе провайдера услуг мультисервисной связи Интернет, включая данные о входящих и исходящих сигналах соединения абонентских аппаратов (терминалов) конкретных пользователей» [11]. На основе этого можно предположить, что получение информации другими электронными способами с применением информационно-аналитических технологий не требует наличия судебного решения.

С исключением из области оборота цифровой информации способов ее сбора при наличии

судебного решения, предусмотренных ФЗ «Об ОРД» необходимо рассмотреть случаи ограничения получения такой информации другими федеральными законами («О банках и банковской деятельности» и «О коммерческой тайне»).

Федеральный закон «О банках и банковской деятельности» от 2 декабря 1990 г. № 395-1 в ч. 1 ст. 26 определяет перечень объектов, на которые распространяется банковская тайна [12]. Она гарантирует тайну об операциях, о счетах и вкладах клиентов и корреспондентов. В соответствии с ч. 5 этой же статьи оперативные подразделения могут получить сведения по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц только на основании судебного решения.

Вместе с тем согласно чч. 2, 4 ст. 26 информация, выдаваемая оперативно-разыскным органам по судебному решению, предоставляется при наличии согласия руководителя следственного органа органам предварительного следствия по делам, находящимся в их производстве без судебного решения. Так же в соответствии с ч. 2 этой же статьи федеральные и арбитражные суды (судьи), Счетная палата Российской Федерации, Федеральная налоговая служба Российской Федерации, Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации и Федеральная служба судебных приставов Российской Федерации вправе получить сведения по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, без каких-либо ограничений на основании лишь соответствующего запроса.

Кроме того, без судебного решения (по запросу) в соответствии со ст. 26, информация по операциям, счетам и вкладам физических лиц выдается руководителям (должностным лицам) федеральных органов государственной власти, перечень которых определяется Президентом Российской Федерации, а также председателю Центрального банка Российской Федерации и высшим должностным лицам субъектов Российской Федерации (руководителям высших исполнительных органов государственной власти субъектов Российской Федерации), Федеральной таможенной службы Российской Федерации и т. д.

Более того, согласно ч. 27 ст. 26 информация об открытии или о закрытии счетов, вкладов (депозитов), об изменении реквизитов счетов, вкладов (депозитов) организаций, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, физических лиц, о предоставлении права или прекращении права организаций и граждан,

осуществляющих предпринимательскую деятельность без образования юридического лица, использовать корпоративные электронные средства платежа для переводов электронных денежных средств, об изменении реквизитов корпоративного электронного средства платежа на постоянной основе в электронном виде сообщается кредитной организацией Федеральной налоговой службе Российской Федерации. Как видим, прослеживается перекос в праве получения сведений между различными государственными органами и службами.

Данное обстоятельство, а именно отсутствие возможности оперативно получить сведения из кредитных организаций в полной мере нивелируют открывающиеся возможности при использовании оперативными подразделениями информационно-аналитических технологий в данном направлении.

Очевидно, что Федеральный закон «О банках и банковской деятельности» требует скорейшего реформирования в части расширения прав оперативных подразделений в доступе к соответствующим сведениям. Это позволит более эффективно использовать передовые достижения в области получения и анализа информации. Тем более что прецедент электронного обмена сведениями между кредитными организациями и налоговыми органами существует, а значит, существует и механизм такого обмена.

Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ определяет, что информацией, составляющей коммерческую тайну, являются сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности. Все они имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны [13].

Вместе с тем в соответствии с ч. 1 ст. 6 обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе данную информацию. При этом мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну.

Исходя из приведенной нормы оперативные подразделения, использующие информационно-аналитические технологии, на законодательном уровне ограничены в праве получения электронным способом доступа к информационным базам данных коммерческих организаций и индивидуальных предпринимателей. Указанное обстоятельство снижает эффективность применения информационно-аналитических технологий.

Полагаем, что Федеральный закон «О коммерческой тайне» нуждается в модернизации. Его стоит дополнить нормами, наделяющими оперативные подразделения правами электронного доступа к информационным базам данных коммерческих организаций и индивидуальных предпринимателей в целях выявления и раскрытия совершенных преступлений.

Таким образом, действующее законодательство Российской Федерации в области применения новейших технологий получения и обработки информации оперативно-разыскными органами нуждается в совершенствовании и существенной доработке. Вслед за изменениями, происходящими в обществе, связанными с развитием информационно-аналитических технологий, постоянного реформирования требует нормативно-правовая база, регулирующая отношения, которые возникают при их использовании в оперативно-разыскной деятельности.

Примечание

* Исходя из того, что на сегодняшний день для получения, обработки и анализа информации все более широко применяются информационно-аналитические технологии, носящие обособленный характер, по тексту будет использован термин «информационно-аналитические технологии».

Список библиографических ссылок

1. Стратегия развития информационного общества в Российской Федерации: утверждена Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 // Рос. газ. 2008. 16 февр.
2. Осипенко А. Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. 2015. № 2. С. 13—19.
3. Осипенко А. Л., Лахин А. Н. Использование информационных технологий в деятельности оперативных подразделений органов внутренних дел // Вестник Волгоградской академии МВД России. 2016. № 2 (37). С. 101—105.
4. Алексеева А. П., Зуева О. В., Иванов А. С., Кривошеин П. К. Мониторинг общественного мнения как способ оценки деятельности российской полиции // Вестник Волгоградской академии МВД России. 2015. № 4 (35). С. 50—57.
5. Нешко А. Н. Особенности получения доказательственной информации при исследовании компьютерных данных // Судебная экспертиза. 2007. № 1. С. 62—66.
6. Выступление Президента Российской Федерации В. В. Путина на расширенном заседании коллегии МВД России 15 марта 2016 г. URL: <http://www.kremlin.ru> (дата обращения: 20.09.2016).
7. Выступление Министра внутренних дел Российской Федерации В. А. Колокольцева на расширенном заседании коллегии МВД России 15 марта 2016 г. URL: <https://vipk.mvd.rf> (дата обращения: 20.09.2016).
8. Луговик В. Ф., Осипенко А. Л. Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования // Вестник Воронежского института МВД России. 2015. № 4. С. 7—12.
9. Об оперативно-розыскной деятельности: федер. закон от 12 августа 1995 г. № 144-ФЗ (в ред. от 6 июля 2016 г.) // СЗ РФ. 1995. № 33. Ст. 3349.
10. О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России: приказ МВД России от 19 июня 2012 г. № 608 // Рос. газ. 2012. 3 авг.
11. Смагоринский Б. П., Вехов В. Б., Мартынов А. Н. Особенности расследования изготовления и оборота материалов с порнографическими изображениями несовершеннолетних, совершенных с использованием информационно-телекоммуникационных технологий // Вестник Волгоградской академии МВД России. 2012. № 1 (20). С. 159—165.
12. О банках и банковской деятельности: федер. закон от 2 декабря 1990 г. №395-1 (в ред. от 3 июля 2016 г.) // СЗ РФ. 1996. № 6. Ст. 492.
13. О коммерческой тайне: федеральный закон от 29 июля 2004 г. № 98-ФЗ (в ред. от 12 марта 2014 г.) // СЗ РФ. 2004. № 32. Ст. 3283.

© Лахин А. Н., 2016