

Таким образом, обеспечение безопасности участников уголовного процесса является важным направлением по преодолению противодействия раскрытию и расследованию преступлений, поскольку от степени их защищенности зависит, насколько объективными и достоверными будут даваемые ими на предварительном следствии и в суде показания. Подтверждением этого является практика применения мер безопасности в отношении свидетелей и потерпевших, поскольку именно эти участники уголовного процесса в большей степени подвергаются негативному воздействию со стороны субъектов противодействия.

УДК 343.14

*И.В. Литвинова*

### **СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ НОРМ ЗАКОНОДАТЕЛЬСТВА РОССИИ И БЕЛАРУСИ О ДОПУСТИМОСТИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ**

В последнее время сотрудники правоохранительных органов все чаще сталкиваются с необходимостью использования в доказывании компьютерной информации, или так называемых электронных доказательств. Электронная переписка, текстовые файлы, файлы с видео-, аудиозаписями и изображениями часто становятся важными доказательствами при расследовании преступлений, причем не только преступлений в сфере компьютерной информации, но и любых других. Их значение особенно возрастает в тех случаях, когда других прямых доказательств (показания свидетелей, вещественные доказательства, иные документы) получить в ходе предварительного расследования и проведенных оперативно-розыскных мероприятий не удалось.

Несмотря на это, вопрос о допустимости электронных доказательств все еще не урегулирован нормами российского уголовно-процессуального законодательства. Так, оценка допустимости компьютерной информации до настоящего времени проводится по критериям, разработанным для традиционных видов доказательств, в том числе об известности их источника и соблюдении процедуры их получения. Однако установить первоначальный источник компьютерной информации представляется возможным далеко не во всех случаях, а процедура ее изъятия в какой-то мере закреплена российским законодателем только применительно к уголовным делам в сфере экономики: ст. 164<sup>1</sup> УПК РФ содержит требование об обязательном участии специалиста в изъятии электронных носителей информации, а также запрет их изъятия, за исключением случаев, когда такое изъятие производится на основании решения суда, либо для производства уже назначенной судебной экспертизы в отношении электронных носителей информации, либо если на обнаруженных электронных носителях содержится информация, полномочиями на хранение и использование которой лицо не обладает, или которую может использовать для совершения новых преступлений, или если ее копирование может повлечь за собой ее повреждение либо утрату. В практической деятельности такое положение дел приводит к тому, что допустимость электронных доказательств ставится под сомнение только из-за способа их получения.

Не определен в российском уголовном процессе и статус электронных доказательств – они не отнесены законодателем ни к одному из традиционных видов доказательств, таких как вещественные доказательства или иные документы, и не выделены в отдельный самостоятельный вид. Ст. 84 УПК РФ относит к иным документам иные носители информации, но не саму компьютерную информацию, тем не менее последняя в настоящее время в практической деятельности, как правило, признается иным документом. Что касается УПК Республики Беларусь, то он в ч. 2 ст. 88 содержит положения, аналогичные российскому законодательству. Однако следует обратить внимание на тот факт, что доказательственное значение по уголовному делу имеет именно содержание компьютерной информации, а не ее носитель. К тому же свойства компьютерной информации позволяют легко перенести ее на другой носитель без потери ее свойств и содержания, а также удалить ее с исходного носителя. В связи с этим полагаем нелогичным признавать доказательством не саму информацию, а ее электронный носитель.

Что касается требований к порядку изъятия и осмотра электронных доказательств, то в этой области уголовно-процессуальное законодательство Республики Беларусь содержит более прогрессивные положения по сравнению с законодательством Российской Федерации. Так, п. 14 ч. 5 ст. 34 УПК Республики Беларусь закрепляет полномочия прокурора санкционировать проведение осмотра компьютерной информации. Ч. 3<sup>1</sup> ст. 204 УПК Республики Беларусь регламентирует порядок действий в случае невозможности либо нецелесообразности изъятия объекта, содержащего компьютерную информацию, закрепляя возможность ее копирования при обеспечении условий, исключающих возможность ее утраты, использовании процедур и методов, обеспечивающих действительность копируемой компьютерной информации. Дополнительно в ч. 5 указанной статьи отмечается право следователя привлечь к участию в осмотре не только специалиста, но и подозреваемого, обвиняемого, потерпевшего и свидетеля. Ст. 204<sup>1</sup> УПК Республики Беларусь отдельно посвящена процедуре осмотра компьютерной информации. При этом в отличие от российского законодательства положения указанной статьи довольно подробно регламентируют данную процедуру. Прежде всего обращает на себя внимание требование законодателя о необходимости получения согласия на осмотр компьютерной информации, доступ к которой осуществляется посредством аутентификации пользователя либо которая содержит информацию о частной жизни лица, а также сведений, составляющих охраняемую законом тайну, или иной информации, распространение которой ограничено, обладателя этой информации и проведения осмотра в его присутствии. При этом если изъятие компьютерной информации было санкционировано прокурором, то на ее осмотр дополнительная санкция не требуется. Учтена законодателем и такая ситуация, в которой невозможно получение вышеуказанного согласия на осмотр: в случаях, не терпящих отлагательства, осмотр компьютерной информации может быть проведен по постановлению следователя (органа дознания) без санкции прокурора, однако с направлением ему в течение 24 ч соответствующего уведомления.

На наш взгляд, закрепление требований к осмотру компьютерной информации в уголовно-процессуальном законодательстве Российской Федерации положительно бы повлияло на регулирование использования в доказывании электронных доказательств, в том числе решение вопроса об их допустимости.