УДК 343.140.02
DOI 10.52452/19931778_2023_6_126

ПРОБЛЕМЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ИЗ ОБЛАЧНЫХ ХРАНИЛИЩ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

В.А. Тимченко

Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского, Н. Новгород

forensacc@mail.ru

Поступила в редакцию 04.09.2023

В настоящее время цифровые технологии все активнее внедряются в различные сферы общественной жизни. Это обстоятельство повлияло и на деятельность по расследованию преступлений. В частности, информация, имеющая доказательственное значение, нередко содержится на электронных носителях, доступ к которым не всегда возможен по ряду объективных и субъективных причин. К числу таких носителей относятся и компьютеры дата-центров различных «облачных» сервисов.

Цель данной работы заключается в исследовании проблем формирования доказательственной базы при расследовании преступлений в условиях цифровизации и глобализации сети Интернет. В статье исследуются проблемные вопросы получения информации, имеющей доказательственное значение, из «облачных» сервисов, дата-центры которых расположены за пределами юрисдикции Российской Федерации.

В ходе исследования использованы методы: сравнительный анализ, систематизация, индукция, дедукция.

Предложены организационные и правовые пути решения проблем получения информации, имеющей доказательственное значение, носителями которой являются различные «облачные» сервисы.

Ключевые слова: облачные хранилища, дата-центры, информация, международные правовые акты, уголовно-процессуальное законодательство, правовая регламентация, безопасность.

Современные телекоммуникационные технологии находят самое разнообразное применение в жизни общества. Они существенно облегчают выполнение различных задач и обеспечивают их более быстрое и качественное решение. Вместе с тем они все активнее используются в процессе осуществления преступной деятельности на всех ее этапах: приготовления к совершению преступления, его совершения и сокрытия следов совершенного преступления.

К сожалению, приходится констатировать, что действующее законодательство существенно отстает от потребностей предотвращения, пресечения и раскрытия преступлений с использованием высоких технологий. В этой связи нельзя не согласиться с тем, что «стремительное развитие информационно-телекоммуникационных технологий, появление новых информационно-технических средств кардинально изменило жизнь общества в целом, а также отдельно жизнь каждого человека. Вместе с тем ускоренный темп развития подобных технологий явился детерминантом совершенствования преступности. В настоящее время все чаще электронные средства и информация становится способами совершения общественно опасных посягательств» [1, с. 108].

Одной из наиболее острых проблем при расследовании преступлений является получение доказательственной информации из так называемых облачных хранилищ. Фактически в роли облачных хранилищ выступают мощные серверы дата-центров, физически находящиеся в различных точках земного шара, доступ к которым у пользователя может быть круглосуточным в режиме онлайн с использованием Интернета. При этом информация пользователя в виде фрагментарных файлов может быть размещена одновременно на нескольких мощных компьютерах, объединенных в одну виртуальную сеть.

Дата-центры могут находиться не на территории Российской Федерации и, соответственно, не входить в ее юрисдикцию. Естественно, это обстоятельство существенно осложняет получение информации из облачных хранилищ при расследовании преступлений. Например, компания хранит свои данные бухгалтерского, налогового и складского учета и отчетности в облачном хранилище (что законом не запрещено). Дата-центры данного облачного хранилища находятся за пределами территории Российской Федерации. Возникает вопрос, как получить данную информацию при расследовании преступления экономической направленности, если организация, в отношении которой проводится расследование, отказывается добровольно выдать эту информацию. Причем международных соглашений по выдаче такой информации, ратифицированных Российской Федерацией, нет.

Существуют различные виды облачных хранилищ. Как отмечают исследователи, «к сервисам как к источникам криминалистически значимой информации, которые содержат в себе признаки облачных хранилищ данных, можно отнести: 1) социальные сети и мессенджеры: Telegram, WhatsApp Cloud, Discord, Facebook, GroupMe, IMO, Instagram, Line, Skype, SkyPixel, Slack, TamTam, TikTok и т.д.; 2) облачные хранилища: Grindr Google Backup, MEGA, Box, inCloud Drive, OneDrive, Yandex Disk и т.д.; 3) сервисы электронной почты: Google Mail, Mail (IMAP), Mail.Ru Mall, Yandex Mail, SecMail»[1] [2, с. 216].

Как видно из данного перечня, большинство существующих облачных хранилищ не являются отечественными. Следовательно, и дата-центры, в которых хранится «облачная» информация, расположены за пределами Российской Федерации.

Принципиальная возможность получения информации из облачных хранилищ существует. Как отмечает В.Ю. Шефер, «в данный период времени для извлечения криминалистической значимой информации в «облачных» сервисах существуют специализированные программные комплексы, которые позволяют извлечь информацию без повреждения и внесения изменений в объект исследования. Безопасное извлечение данных из облачных хранилищ требует специальных познаний. Оно выполняется как процесс выполнения извлечения информации из компьютеров или мобильных устройств, так как данные хранятся на удаленных серверах, что сильно затрудняет исследование значимой информации» [3, с. 145].

Вышеназванными возможностями обладает, например, программный комплекс «Мобильный криминалист». Конечно, можно получить криминалистически значимую информацию и при осмотре компьютера. Как отмечают О.Н. Кисилев и А.А. Черноперов, «рассмотрев только основные места, в которых операционная система хранит сведения о своей работе и взаимодействии с другими системами, устройствами и пользователями, можно убедиться в том, что тщательный осмотр и анализ содержания реестра системы и системных журналов позволяет получить значительный объем информации, как непосредственно имеющей доказательственное значение, так и ориентирующей для дальнейшего планирования и производства следственных действий» [4, с. 44]. Однако такую информацию можно получить только имея в своем распоряжении компьютер, на котором хранилась интересующая следствие информация или совершались операции. Что же касается получения информации, хранящейся в облачных сервисах, то осмотреть компьютер весьма проблематично, поскольку физически он может находиться за пределами юрисдикции Российской Федерации.

В этой связи нельзя не согласиться с С.В. Зуевым и В.С. Черкасовым, которые указывают, что «участником информационного взаимодействия в киберпространстве может быть лицо, находящееся в любой точке планеты Земля, а программно-аппаратные средства могут быть физически расположены на территории одного или одновременного неограниченного количества государств» [5, с. 17].

Естественным путем решения данной проблемы должно быть принятие соответствующих международных нормативных правовых актов. Например, одним из таких действующих актов является Конвенция о преступности в сфере компьютерной информации ETS № 185 от 23 ноября 2001 года. Однако некоторые условия данной конвенции противоречат интересам Российской Федерации, поэтому она нашей страной не ратифицирована. Кроме того, исходя из содержания этой конвенции, она направлена на противодействие преступности именно в сфере создания и использования компьютерной информации. Вместе с тем преступления могут быть совершены не только в сфере компьютерной информации, а, например, в сфере экономической деятельности. Однако экономическая информация, которая могла бы послужить доказательством по уголовному делу, хранится в электронном виде, т.е. на компьютерах, включая дата-центры облачных сервисов. Поэтому принципиальное значение имеет возможность получения любой информации, необходимой в связи с расследованием преступлений, независимо от того, где, в какой юрисдикции она хранится. В настоящее время получение такой информации весьма проблематично. Мы разделяем мнение А.Л. Осипенко и В.Ф. Луговика о том, что «разработчики программного обеспечения и поставщики сетевых услуг, находящиеся в зарубежной юрисдикции, не всегда заинтересованы в сотрудничестве с российскими правоохранительными органами, в результате чего нередко возникают существенные сложности организационного порядка при обращении к ним с запросами на оказание помощи в доступе к данным» [6, с. 65].

Таким образом, альтернативы принятию соответствующей международной конвенции нет. Вместе с тем это процесс длительный и сложный, особенно с учетом характера сегодняшних международных отношений. Как справедливо указывают Е.Р. Россинская и Т.А. Сааков, «процесс реализации новой Конвенции после её принятия, очевидно, будет требовать достаточ-

но большого количества времени, т. к. Конвенция может быть воплощена в жизнь странами-участницами только при условии, если нормы национального законодательства государств не будут препятствовать реализации Конвенции о сотрудничестве в сфере противодействия информационной преступности» [7, с. 116].

Не урегулирован должным образом процесс получения информации из облачных хранилищ и отечественным уголовно-процессуальным законодательством. В этой связи мы разделяем точку зрения Р.В. Костенко и О.А. Петровой, которые справедливо указывают на то, что «на сегодняшний день особенности, связанные с изъятием или копированием информации, хранящейся в «облачном хранилище», не закреплены на законодательном уровне. Сложность заключается в том, что получение такой информации может вызывать затруднения, поскольку чаще всего серверы, на которых хранится эта информация, физически находятся на удалённом расстоянии» [8, с. 66].

В принципе, получить информацию из облачных хранилищ можно используя специальные аппаратно-программные средства, однако и для этого необходимое законодательное обеспечение отстает от требований сегодняшнего дня. Мы разделяем точку зрения А.Л. Осипенко о том, что «требуется более четкая определенность в правовой регламентации применения специальных программных и программно-аппаратных средств, способных обеспечить оперативный доступ к компьютерным данным, представляющим интерес для раскрытия преступлений» [9, с. 48].

Информацию, полученную с помощью соответствующих программно-аппаратных средств, в дальнейшем необходимо использовать для целей доказывания, и поэтому она должна отвечать требованиям, предъявляемым уголовно-процессуальным законодательством к доказательствам, и прежде всего требованию допустимости. Поэтому мы не можем не согласиться с мнением И.П. Можаевой и Е.П. Шульгина относительно проблемы получения процессуально допустимой информации из облачных хранилищ: « ...перед правоохранительными органами встает вопрос обнаружения, доступа, изъятия представляющей доказательственное значение информации и, главное, правильного процессуального оформления данных действий» [10, с. 166].

Таким образом, решение проблемы получения доказательственной информации из облачных хранилищ невозможно без совершенствования действующего уголовно-процессуального законодательства. И начинать решение этой проблемы необходимо с определения характера такого носителя доказательственной информации, как облачное хранилище. Как справедливо отметили В.С. Удовиченко и С.А. Сорокина, «открытым остается вопрос, к какому виду доказательств будет отнесена информация, хранящаяся не в самой памяти электронного носителя, а в облачном хранилище, так называемом облаке смартфонов или других устройств. ... Фактически доступ к такой информации возможен только при подключении к сети Интернет, но в этом случае исследование информации выходит за пределы изъятого объекта (сотового телефона, ноутбука, планшета и др.), поэтому изъятие данного объекта у лица необязательно в связи с тем, что доступ в Интернет можно осуществить с любого другого устройства» [11, с. 134].

Наряду с необходимостью совершенствования уголовно-процессуального законодательства, для решения проблемы получения информации из дата-центров, в которых хранится «облачная» информация, необходимо, по нашему мнению, на законодательном уровне запретить в Российской Федерации пользоваться облачными сервисами, дата-центры которых расположены вне юрисдикции Российской Федерации. Этот запрет может быть временным, до принятия и ратификации международных соглашений, которые бы обязывали страны-участницы этого соглашения беспрепятственно предоставлять информацию из дата-центров облачных сервисов. В противном случае проблема получения информации из дата-центров облачных сервисов решена в ближайшее время не будет.

Сложившаяся ситуация несет непосредственную угрозу безопасности Российской Федерации, в том числе экономической безопасности. В «облаке» может храниться экономическая информация организаций и предпринимателей, необходимая при расследовании уголовных дел экономической направленности, например по налоговым преступлениям. Невозможность получения такой информации приведет к проблемам с формированием доказательств по уголовным делам и, как следствие, позволит виновным избежать ответственности. Государственному и муниципальным бюджетам при этом будет нанесен ущерб, что в конечном итоге создаст условия для ослабления экономической безопасности Российской Федерации. Аналогичная ситуация будет возникать в связи с невозможностью формирования полноценной доказательственной информации и по другим категориям преступлений.

Таким образом, для решения проблемы получения информации из облачных хранилищ при расследовании преступлений необходимо выполнить одновременно два условия:

1. Запретить использование облачных сервисов, дата-центры которых находятся за пределами юрисдикции Российской Федерации;

2. Внести необходимые изменения в уголовно-процессуальное законодательство, направленные на беспрепятственное получение информации из облачных хранилищ в связи с расследованием преступлений.

Примечание

1. Facebook, Instagram принадлежат компании Meta, признанной экстремистской организацией в РФ.

Список литературы

1. Костенко Р.В., Шипицына В.В., Петрова О.А. Изъятие уголовно-процессуальных доказательств в цифровую эпоху // Юридический вестник Кубанского государственного университета. 2022. № 3. С. 105–112.

2. Мамонтов А.Г. Тактические особенности сбора цифровых доказательств в облачном хранилище информации // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2022. № 22-1. С. 216–217.

3. Шефер В.Ю. Основные принципы исследования криминалистически значимой информации в «облачных» сервисах // Экспертные чтения на Енисее: Материалы региональной (межвузовской) научно-практической конференции. Вып. 2. Красноярск: Красноярский государственный аграрный университет, 2021. С. 144–146.

4. Кисилев О.Н., Черноперов А.А. Криминалистически значимая информация в служебных файлах, формируемых операционными системами // Право и закон. 2022. № 4. С. 36–45.

5. Зуев С.В., Черкасов В.С. Действие уголовно-процессуального закона в «киберпространстве»: проблема трансграничных следственных действий // Вестник Южно-Уральского государственного университета. Серия: Право. 2019. Т. 19. № 1. С. 17–23.

6. Осипенко А.Л., Луговик В.Ф. Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений // Общество и право. 2021. № 2 (76). С. 60–68.

7. Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123.

8. Костенко Р.В., Петрова О.А. Проблемы изъятия электронных носителей информации в отечественном уголовном процессе // Юридический вестник Кубанского государственного университета. 2021. № 1. С. 62–71.

9. Осипенко А.Л. Сбор информации и полицейские операции по противодействию организованной преступности в киберпространстве: зарубежный опыт // Общество и право. 2021. № 1 (75). С. 47–55.

10. Можаева И.П., Шульгин Е.П. О понимании доказательств в правоохранительной деятельности в эпоху цифровых преобразований // Юристъ-Правоведъ. 2022. № 4 (103). С. 162–167.

11. Удовиченко В.С., Сорокина С.А. Особенности изъятия информации с электронных носителей в досудебном производстве // Алтайский юридический вестник. 2021. № 2 (34). С. 133–138.

PROBLEMS OF OBTAINING INFORMATION FROM CLOUD STORAGE IN THE INVESTIGATION OF CRIME

V.A. Timchenko

Currently, digital technologies are increasingly being introduced into various spheres of society. This circumstance also affected the activity of investigating crimes. In particular, information of probative value is often contained on electronic media, access to which is not always possible for a number of objective and subjective reasons. These media also include computers in data centers of various «cloud» services.

The purpose of this work is to study the problems of forming an evidence base in the investigation of crimes in the context of digitalization and globalization of the Internet. The article explores the problematic issues of obtaining information of evidentiary value from «cloud» services, the data centers of which are located outside the jurisdiction of the Russian Federation.

Methods used: comparative analysis, systematization, induction, deduction.

Organizational and legal ways of solving the problems of obtaining information of probative value, the carriers of which are various «cloud» services, are proposed.

Keywords: cloud storage, data centers, information, international legal acts, criminal procedure legislation, legal regulation, security.

References

1. Kostenko R.V., Shipitsyna V.V., Petrova O.A. Seizure of criminal procedural evidence in the digital age // Legal Bulletin of the Kuban State University. 2022. № 3. P. 105–112.

2. Mamontov A.G. Tactical features of collecting digital evidence in the cloud storage of information // Actual problems of combating crimes and other offenses. 2022. № 22-1. P. 216–217.

3. Schaefer V.Yu. Basic principles of research of criminalistically significant information in «cloud» services // Expert readings on the Yenisei: Materials of the regional (interuniversity) scientific and practical conference. Issue 2. Krasnoyarsk: Krasnoyarsk State Agrarian University, 2021. P. 144–146.

4. Kisilev O.N., Chernoperov A.A. Criminally significant information in service files generated by operating systems // Right and Law. 2022. № 4. P. 36–45.

5. Zuev S.V., Cherkasov V.S. The effect of the criminal procedure law in «cyberspace»: the problem of cross-border investigative actions // Bulletin of the South Ural State University. Series: Law. 2019. Vol. 19. № 1. P. 17–23.

6. Osipenko A.L., Lugovik V.F. Problems of access of law enforcement agencies to hidden computer information when solving crimes // Society and law. 2021. № 2 (76). P. 60–68.

7. Rossinskaya E.R., Saakov T.A. Problems of collecting digital traces of crimes from social networks and messengers // Criminalistics: yesterday, today, tomorrow. 2020. № 3 (15). P. 106–123.

8. Kostenko R.V., Petrova O.A. Problems of seizure of electronic media in domestic criminal proceedings // Law Bulletin of the Kuban State University. 2021. № 1. P. 62–71.

9. Osipenko A.L. Information gathering and police operations to counter organized crime in cyberspace: foreign experience // Society and Law. 2021. № 1 (75). P. 47–55.

10. Mozhaeva I.P., Shulgin E.P. On understanding evidence in law enforcement in the era of digital transformations // Lawyer-jurist. 2022. № 4 (103). P. 162–167.

11. Udovichenko V.S., Sorokina S.A. Features of information withdrawal from electronic media in pre-trial proceedings // Altai Legal Bulletin. 2021. № 2 (34). P. 133–138.