УДК 343.140.02:344.633:004.738.5 https://doi.org/10.24158/tipor.2017.6.29

Буцкова Оксана Игоревна

адъюнкт
Нижегородской академии МВД России

Butskova Oksana Igorevna

Postgraduate student,
Nizhny Novgorod Academy of
the Ministry of Internal Affairs of Russia

КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ ЗАЯВИТЕЛЯ КАК ПРЕПЯТСТВИЕ ПРИНЯТИЮ ЗАКОННОГО РЕШЕНИЯ НА СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА О ХИЩЕНИЯХ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ ГРАЖДАН, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ СРЕДСТВ СВЯЗИ, СЕТИ ИНТЕРНЕТ

CONFIDENTIALITY OF THE APPLICANT'S PERSONAL DATA AS AN OBSTACLE TO A LAWFUL DECISION ADOPTION AT THE STAGE OF INITIATING A CRIMINAL CASE ON MONEY EMBEZZLEMENT FROM CITIZENS' BANK ACCOUNTS COMMITTED WITH THE HELP OF COMMUNICATION FACILITIES, THE INTERNET

Аннотация:
В статье обсуждается проблематика проведения проверки по сообщениям о хищениях денежных средств с банковских счетов граждан, совершаемых с использованием средств связи. На основе анализа позитивного законодательства и практики его применения автор формулирует предложения по оптимизации процедуры получения информации о персональных данных.

Ключевые слова:
персональные данные, субъект персональных данных, банковская тайна, конфиденциальная информация, сроки проверки сообщения о преступлении, мотивированный запрос.

Summary:
The article discusses the problems of verifying the reports on money embezzlement from citizens' bank accounts committed with the help of communication facilities. Based on the analysis of positive legislation and practice of its application, the author formulates proposals for optimizing the procedure for obtaining information about personal data.

Keywords:
personal data, personal data subject, bank secrecy, confidential information, time limits for verification of a crime report, motivated request.

Возможности сети Интернет практически безграничны, что в негативном смысле делает данную среду площадкой для интернет-преступности. Таким же образом практически мгновенная передача информации с использованием средств сотовой связи с возможностью удаленного доступа обозначила границы телефонной преступности. По данным Банка России, в 2016 г. было совершено около 297 тыс. незаконных операций с использованием банковских карт, эмитированных в России, похищено более 1 млрд р. В среднем хищения совершаются через Интернет и средства сотовой связи и все меньше – через банкоматы и терминалы в магазинах. Количество несанкционированных операций только выросло (в 2015 г. – 261 тыс.) на фоне роста операций с картами (на 30 % в 2016 г.) и совершенствования технологий, используемых преступниками. Из-за малых похищенных сумм (до 5000 р.) пострадавшие часто предпочитают не обращаться с заявлением в полицию. Всего за 2016 г. Банк России зафиксировал 717 несанкционированных операций на общую сумму 1,89 млрд р. [1].

На сегодняшний день проблема сложности расследования данного вида преступлений остается открытой, несмотря на множественные научные исследования в данной области, в которых данный вид преступления рассматривается в рамках криминалистического аспекта, но упускается важная связь с уголовно-процессуальным. Главную сложность составляет своевременное формирование качественной доказательственной базы по данным уголовным делам, основа которой формируется именно на стадии возбуждения уголовного дела в ходе работы должностных лиц органов следствия и дознания.

На стадии возбуждения уголовного дела следователь, орган дознания осуществляют комплекс действий по приему, регистрации сообщения о преступлении, проверке и принятию законного решения. Согласно ст. 145 УПК РФ, по результатам рассмотрения сообщения о преступлении орган дознания, дознаватель, следователь, руководитель следственного органа принимает одно из следующих решений: 1) о возбуждении уголовного дела; 2) об отказе в возбуждении уголовного дела; 3) о передаче сообщения по подследственности [2]. Задача следователя, соответственно, найти или опровергнуть наличие данных, указывающих на признаки преступления.

Проанализированная правоприменительная практика районных отделов полиции говорит о том, что при реализации предписаний процессуального закона на стадии возбуждения уголовного

дела о хищениях денежных средств с банковских счетов граждан, совершаемых с применением средств связи, сети Интернет, нередко допускаются ошибки с нарушением процессуального срока, несоблюдением процессуальной формы, влекущие за собой необоснованные решения и утрату доказательственной ценности полученных сведений. Как правило, первоначальной информации, содержащейся в заявлении, недостаточно для правильной квалификации деяния и принятия обоснованного решения о возбуждении уголовного дела. Решение о возбуждении уголовного дела о хищениях денежных средств с банковских счетов граждан, совершаемых с применением средств связи, сети Интернет, практически никогда не принимается в срок – в течение 3 суток. И на это есть разумные причины. В большинстве случаев для принятия законного и обоснованного решения срок проверки продлевается до 30 суток в связи с истребованием информации по совершенным операциям из банков, компаний сотовой связи, интернет-провайдеров. Но и данного месячного срока бывает недостаточно. Стоит разобраться, почему возникает такая ситуация.

Прежде всего на стадии возбуждения уголовного дела при расследовании преступлений указанного вида в заявлении и объяснении заявителя указываются данные о принадлежащем ему абонентском номере, номере банковского счета, а также данных аккаунта в социальных сетях (в зависимости от способа совершенного преступления). В случае хищений денежных средств с банковского счета гражданина заявитель зачастую предоставляет лишь поверхностные сведения совершенного преступления. Для установления обстоятельств, указывающих на признаки преступления, личности и местонахождения преступника, необходимы конкретные данные, а именно абонентский номер звонившего, банковский счет, на который переведены похищенные денежные средства, и иная информация. При установлении указанных данных нельзя обойтись без содействия банков, компаний сотовой связи, интернет-провайдеров. Именно поэтому дальнейшие действия направлены на получение указанных сведений посредством направления мотивированных запросов следователем. Можно возразить, что заявитель и сам имеет возможность истребовать выписки из банковских организаций и компаний сотовой связи, но зачастую в них нет части той информации, которая предоставляется следователю по его мотивированному запросу.

Банковские учреждения и компании сотовой связи отказываются предоставлять информацию по запросам должностных лиц без судебного решения в том случае, если отсутствует возбужденное уголовное дело. Что касается банков, это не вполне соответствует букве закона, так как в соответствии со ст. 26 федерального закона «О банках и банковской деятельности» [3] справки по счетам и вкладам физических лиц выдаются кредитной организацией при наличии согласия руководителя следственного органа органам предварительного следствия по делам, находящимся в их производстве. Интерпретировать данную норму можно по-разному, так как в ней нет конкретного указания на «уголовное» дело. Банки трактуют эту норму в свою пользу, не принимая во внимание, что на рассмотрении у следователей находятся и материалы проверки сообщения о преступлении, поэтому стоит конкретизировать, чтó законодатель имел в виду, не указывая конкретного понятия «уголовное дело». Согласно этой же норме, должностным лицам органов, уполномоченных осуществлять оперативно-разыскную деятельность, указанная информация выдается также на основании судебного решения. В связи с этим должностное лицо, которое проводит предварительную проверку, в трехдневный срок не имеет реальной возможности получить судебное решение по своему мотивированному ходатайству о разрешении проведения соответствующих мероприятий. Соответственно, практически всегда происходит продление срока предварительной проверки сообщения об указанных преступлениях до 30 суток.

Рассматривая законодательную основу конфиденциальности сведений, запрашиваемых следователем из компаний сотовой связи, стоит отметить, что даже при наличии возбужденного уголовного дела для получения указанных сведений необходимо судебное решение. В своем отказе на предоставление указанной информации компании сотовой связи ссылаются на положения Конституции РФ, требования ст. 7 ФЗ «О персональных данных», ст. 63 ФЗ «О связи». В соответствии с последней, сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям [4]. В данном случае заявитель может являться непосредственным отправителем указанных сообщений, поэтому имеет законное право на получение информации.

На нарушение следователями положений ст. 7 ФЗ «О персональных данных» ссылаются представители компаний сотовой связи, операторы и иные лица, получившие доступ к персональным данным. Согласно этой статье, представители компаний сотовой связи и др. обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных [5]. Таким образом, заявитель, являясь субъектом персональных данных, имеет право дать согласие на раскрытие персональной информации третьему лицу, которым может являться следователь.

Также необходимо обратить внимание на установленные в данном законе сроки исполнения запроса субъекта персональных данных. В ст. 14 ФЗ «О персональных данных», в которой отражено право субъекта персональных данных на доступ к ним, установлено, что по общему правилу ответ оператора должен быть предоставлен не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса. В этом случае необходимость получения такого ответа на запрос в рамках предварительной проверки сообщения о преступлении отпадает, так как ответ в любом случае не приходит в срок, отведенный для указанной проверки. Представляется возможным и целесообразным сократить срок ответа оператора хотя бы до 20 суток. В этом случае возможно избежать процессуальных и практических недочетов.

Следует отметить, что компании сотовой связи защищают персональные данные клиентов от органов предварительного расследования очень тщательно, но не в состоянии защитить указанные данные от своих сотрудников. В Иркутской области сотрудник компании сотовой связи передавал мошенникам данные клиентов. В результате мошеннических действий 10 граждан лишились более 100 тыс. р., которые похитили мошенники. Именно из-за таких происшествий в 2017 г. Роскомнадзор намерен проверить, как крупнейшие сотовые операторы выполняют Закон о хранении персональных данных. В список тех, кого проверят в плановом порядке, попали Мегафон, МТС [6]. Плановые проверки по выполнению требований о хранении персональных данных ждут 12 IT- и интернет-компаний. В список попали такие известные компании, как «Microsoft Россия», «ВКонтакте» и «Озон» (ООО «Интернет Решения»), Samsung (ООО «Самсунг Электроникс Рус Компани») и Hewlett-Packard (HP, ЗАО «Хьюлетт-Паккард А.О.») [7]. Всего же будет проведено несколько тысяч проверок организаций, которые запрашивают и обрабатывают персональные данные пользователей. Также с 1 июля 2017 г. усилена административная ответственность за нарушения законодательства в области персональных данных, за невыполнение оператором предусмотренной законодательством в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных [8].

В связи в вышесказанным целесообразно предложение, которое в некотором роде упрощает процедуру получения информации из компаний сотовой связи, банков, интернет-компаний. Необходимо рассмотреть возможность упразднения процедуры получения разрешения суда на истребование данного рода информации от соответствующих организаций. В настоящее время в УПК РФ предусмотрен аналогичный правовой механизм при осмотре жилища с согласия проживающих в нем лиц без судебного решения. Таким образом, получение судебного решения до возбуждения уголовного дела возможно было бы исключить в том случае, если заявитель даст письменное согласие на получение следователем информации об операциях по банковским счетам и вкладам заявителя, о входящих и исходящих сигналах соединений телефонного аппарата заявителя. Фактически его права как клиента указанных организаций и права, предусмотренные ст. 23 Конституции РФ [9], нарушены не будут, так как неправомерного доступа к указанной информации нет. Соответственно, полученная в разумный срок информация по материалу проверки будет способствовать принятию обоснованного решения о возбуждении уголовного дела должностным лицом.

Все это приведет к результативности и законности при проведении предварительной проверки на стадии возбуждения уголовного дела о хищениях денежных средств с банковских счетов граждан, совершаемых с применением средств связи, сети Интернет без нарушений положений Конституции РФ.

Ссылки:

1. Зубков И. Хакнули миллиард [Электронный ресурс] // Российская газета. 2017. № 7200 (34). URL: https://rg.ru/2017/02/15/hakery-za-god-sovershili-okolo-300-tysiach-hishchenij-s-bankovskih-kart-rossiian.html (дата обращения: 12.03.2017).
2. Уголовно-процессуальный кодекс Российской Федерации : от 18 дек. 2001 г. № 174-ФЗ : ред. от 17 апр. 2017 г.
3. О банках и банковской деятельности : федер. закон от 2 дек. 1990 г. № 395-1 : ред. от 3 июля 2016 г. : с изм. и доп., вступ. в силу с 1 янв. 2017 г.
4. О связи : федер. закон от 7 июля 2003 г. № 126-ФЗ (послед. ред.).
5. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ (послед. ред.).
6. Роскомнадзор проверит сотовые компании в 2017 году [Электронный ресурс] // Российская газета. 2016. 29 дек. URL: https://rg.ru/2016/12/29/roskomndazor-proverit-sotovye-kompanii-v-2017-godu.html (дата обращения: 05.05.2017).
7. Шадрина Т. Роскомнадзор предупредил о проверке «ВКонтакте» [Электронный ресурс] // Российская газета. 2016. 11 янв. URL: https://rg.ru/2016/01/11/proverki-site-anons.html (дата обращения: 03.05.2017).
8. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] : федер. закон от 7 февр. 2017 г. № 13-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
9. Конституция Российской Федерации : принята всенародным голосованием 12 дек. 1993 г. : с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30 дек. 2008 г. № 6-ФКЗ, от 30 дек. 2008 г. № 7-ФКЗ, от 5 февр. 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ.

References

‘Roskomnadzor will check cellular companies in 2017’ 2016, *Rossiyskaya gazeta,* December 29, viewed 05 May 2017, <https://rg.ru/2016/12/29/roskomndazor-proverit-sotovye-kompanii-v-2017-godu.html>, (in Russian).

Shadrina, T 2016, ‘Roskomnadzor warned about the verification of VKontakte’, *Rossiyskaya gazeta,* January 11, viewed 03 May 2017, <https://rg.ru/2016/01/11/proverki-site-anons.html>, (in Russian).

Zubkov, I 2017, ‘Someone hacked a billion’, *Rossiyskaya gazeta,* no. 7200 (34), viewed 12 March 2017, <https://rg.ru/2017/02/15/hakery-za-god-sovershili-okolo-300-tysiach-hishchenij-s-bankovskih-kart-rossiian.html>, (in Russian).