DOI: 10.7256/1811-9018.2014.12.13846
При цитировании этой статьи сноска на doi обязательна

Оконенко Р.И.

ИССЛЕДОВАНИЕ ПОРТАТИВНОГО ЭЛЕКТРОННОГО УСТРОЙСТВА В ХОДЕ ОБЫСКА ЗАДЕРЖАННОГО В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ПРАВЕ США: ПОИСК БАЛАНСА ИНТЕРЕСОВ ГРАЖДАНИНА И ГОСУДАРСТВА

Аннотация: *В статье описываются основанные проблемы, с которыми сталкиваются судебные органы США при исследовании портативных цифровых устройств задержанных, анализируется отличия современных информационных технологий от обычных контейнеров, на основании чего делается вывод о неприменимости традиционных для американского права юридических стандартов к электронным носителям персональных данных. Особое внимание уделяется анализу решения Верховного суда США от 25 июня 2014 года, которое признает сотовый телефон особо значимым личным предметом, обыск которого допускается только на основании отдельного судебного ордера. Автор также описывает основные точки зрения американских правоведов по вопросу о том, до какого предела возможно исследование портативного цифрового устройства задержанного, с тем, чтобы соответствующее действие сотрудника правоохранительного органа отвечало как публичным интересам борьбы с преступностью, так и частному интересу конкретного гражданина, выражающимся в сохранности значимой личной информации. Основной общенаучный метод данного исследования – системный подход, поскольку в статье показывается, как появление новых технологий влияет на общественные отношения, которые видоизменяясь, нуждается в новом режиме регулирования. Значительное место в методологии уделено синтезу – поскольку правовые нормы здесь сопоставляются с элементами социальной реальности (интересами граждан, задачами правоохранительной деятельности и так далее). Основной вывод исследования состоит в несводимости современных устройств передачи данных к простым контейнерам, из чего ранее исходили американские суды различных уровней. В более обобщенном виде итог работы видится в доказывании необходимости установления для современных информационных технологий особого процессуального статуса, учитывающего их особенности, прежде всего, как объекта защиты прав граждан на тайну личной жизни.*

Abstract: *This article describes the main problems, which the US courts face while examining the portable digital devices of arrestees, and analyzes the differences between the modern information technologies and conventional methods of storing information (planner, briefcase, etc.). This leads to the conclusion that the American legislation is unable to implement the traditional legal standards towards the electronic carriers of personal data. A special attention is given to the analysis of the decision of the United States Supreme Court from June 25th 2014, which finds mobile phones to be a significant personal object, and their search can only be conducted based on a separate court warrant. The author also describes the key points of view of American legislators on the question of to what extent can an examination of a portable digital device of a suspect be conducted by a member of law enforcement in order to address both, the public interest of fighting crime and private interest of a citizen by protecting the important personal information. The main conclusion of the research consist in the incomparability of the modern communication devices to the traditional means of writing down information, which used to be the basis of the work of American courts of all levels.*

Ключевые слова: *Электронные доказательства, цифровые доказательства, защита персональных данных, тайна личной жизни, осмотр компьютера, осмотр сотового телефона, личный обыск, электронный носитель информации, право США, уголовный процесс США.*

Keywords: *Electronic evidence, digital evidence, protection of personal data, personal secrets, search of a computer, examination of a mobile device, pat-down, US law, US criminal process.*

Институт обыска при задержании существует во многих странах мира, в то числе в США и позволяет органам правопорядка получить ценные доказательства криминальной активности гражданина в короткий промежуток времени. Напряженная психологическая обстановка задержания, которая может быть отягчена физическим сопротивлением предполагаемого преступника, быстрота проведения данного процессуального действия, высокая вероятность обнаружения при задержанном ценных доказательств – все это делает нецелесообразным сложную регламентацию указанной операции и предполагает сравнительно простой правовой режим регулирования соответствующего вида деятельности.

Указанная простота, например, проявляется в том, что данный вид обыска в американском праве не подлежит обязательному судебному контролю, то есть может быть проведен без судебной санкции [1, с. 482]. Основные же правила здесь устанавливаются посредством судебных прецедентов и гласят, что граница проводимого обыска должна совпадать с пространством, находящимся под физическим контролем арестованного [3, p. 31]; в ходе обыска допускается открытие обнаруженного при лице контейнера [6, p. 499]; наличие у полицейских правовых оснований для задержания само по себе предполагает право на физическое обследование человека [2, p. 7]; цель обыска состоит в предотвращении опасности для жизни и здоровья полицейского либо в лишении лица возможности уничтожить доказательства [9, p. 1253].

Данные прецедентные правила применялись на практике несколько десятилетий без каких-либо существенных изменений до того момента, пока в жизни американцев не появились сначала пейджеры, потом сотовые телефоны, и, наконец, смартфоны. Принимая как данность то, что любые контейнеры, находящиеся при арестованном, могут быть открыты и обследованы, суды США распространили это

DOI: 10.7256/1811-9018.2014.12.13846
При цитировании этой статьи сноска на doi обязательна

правило и к цифровым коммуникационным устройствам без учета их специфики как средств передачи и обработки личной информации, выраженной в электронной форме [4, p. 568].

Вместе с тем, американская юридическая доктрина уделила значительное внимание недопустимости аналогии между закрытым контейнером и цифровым устройством. Правоведы неоднократно обращали внимание, что современные средства связи могут хранить гораздо более значительный объем разнообразной информации о личной жизни пользователя, чем какой-либо контейнер, а потому деятельность по исследованию электронных устройств должна подлежать адекватному регулированию, включающему расширенный перечень гарантий, направленных на защиту частной тайны.

При этом, чем дальше продвигались технологические новшества, тем более неприглядными начали казаться прецедентные правила, сформулированные в конце 60-х – первой половине 70-х годов прошлого века.

Наконец, 25 июня 2014 года Верховный суд США, рассматривая дело «Riley против California» выработал новый правовой стандарт законности обыска сотового телефона задержанного, что стало существенным шагом вперед на пути выработки процессуальных правил, специально предназначенных для регламентации процедуры исследования портативных электронных устройств [10].

В частности, судьи отметили, что обнаруженное электронное устройство вряд ли может представлять опасность для жизни и (или) здоровья полицейского, потому в данном случае не имеется оснований проводить обыск соответствующей информационной технологии для того, чтобы обезопасить сотрудников правоохранительных органов. Вместе с тем, судьи не исключили, что любое устройство, помимо средства обработки и передачи данных, является еще физическим объектом, который может маскировать средство противодействия задержанию. Учитывая это, Верховный Суд США посчитал разумным признать право полицейского на осмотр устройства как обычного предмета без возможности просмотра хранящейся в нем электронной информации. Довод же представителей штата Калифорния о том, что с помощью портативного цифрового устройства предполагаемый преступник может вызвать помощь и, таким образом, создать опасность для сотрудников правоохранительных органов, был отвергнут судом, поскольку не был обоснован ссылкой на конкретный опыт правоохранительной деятельности [7, p. 322].

Говоря о том, что с помощью сотового телефона задержанный может уничтожить доказательства, Верховный Суд США указал, что для предотвращения указанной опасности полицейским достаточно просто изъять устройство у соответствующего лица без последующего изучения его содержания.

Судьи приняли во внимание, что существуют способы сокрытия или уничтожения цифровых сведений с уже изъятого телефона при помощи удаленного доступа через беспроводную сеть, а также возможность кодирования, то есть настройки телефона таким образом, чтобы, спустя определенное время, доступ к сохраненным на нем сведениям был затруднен. Вместе с тем, суд указал, что кодирование – это не действия арестованного по сокрытию информации от полиции, а техническая особенность определенных моделей телефонов, действующая автоматически, в то же время, проблема удаленного доступа может быть решена способом, не связанным с ущемлением прав граждан на защиту тайны личной жизни путем использования дешевых и простых в обращении технологий (например, алюминиевых чехлов, так называемых «сумок Фарадея», блокирующих поступление на телефон сигналов извне) [8, p. 14].

Несмотря на актуальность всех приведенных рассуждений Верховного Суда США, вероятно, самое важное из них состоит в признании того, что поиск информации на цифровом устройстве не сравним с обыском обычного контейнера, находящегося при задержанном [7, p. 325].

С данными выводами суда трудно не согласиться, поскольку современные возможности цифровых устройств позволяют хранить множество различных видов информации, которая ранее могла храниться только на обычных материальных носителях, занимающих значительное пространство. К примеру, сегодня на смартфоне средней ценовой категории может содержаться личная переписка со множеством различных людей, финансовая документация за периоды времени, исчисляемые годами, не говоря уже о значительном числе фото– и видеоматериалов. В то же время, содержание указанных сведений в аналоговой форме заняло бы несопоставимо больший объем и вывело бы соответствующий контейнер из числа предметов подлежащих быстрому обыску без получения судебного решения, так как указанное хранилище, исходя из своих параметров, просто не могло бы находиться при гражданине.

Второе важное отличие обычных контейнеров от электронных устройств состоит, по мнению суда, в значении словосочетания «содержать в себе». Если физический объект может предоставить на обозрение лишь те данные, что содержит, то электронное устройство является еще и средством коммуникации и потому может получить информацию извне [2, p. 21].

Приняв во внимание указанные отличия, Верховный суд США посчитал, что сотовый телефон задержанного потенциально может содержать настолько значительный объем сведений, что для обеспечения прав граждан на защиту тайны личной жизни, его допускается исследователь лишь после получения отдельного судебного ордера.

Таким образом, особенности информационных технологий были учтены прецедентным правом США для внесения изменений в действующие правовые стандарты.

Принимая во внимание всю ценность вынесенного решения для защиты прав граждан на тайну личной жизни, необходимо отметить некоторые его отрицательные моменты.

Наиболее очевидным недостатком является привязка нового процессуального стандарта к конкретной технологии – сотовому телефону. Хотя по тексту решения видно, что судьи рассуждают о сотовом телефоне, схожем по функциональности с обычным компьютером, они, все-таки, говорят только про определенный класс современных информационных устройств. В то же время, сотовый телефон является лишь временным достижением, на смену которому, бесспорно, придут другие технические новшества. Не исключено, что через пару лет информационные технологии достигнут такого уровня, что их сложно будет назвать «телефонами».

Верно и другое – существует множество переносимых устройств без функции телефона или, к примеру, с небольшим объемом памяти либо без доступа к информационно-телекоммуникационной сети «Интернет». Будут ли такие

DOI: 10.7256/1811-9018.2014.12.13846
При цитировании этой статьи сноска на doi обязательна

устройства подпадать под правило о получении судебного ордера на обыск, неясно, так как судебный запрет касается только определенной технологии совмещающей в себе функции телефона, персонального компьютера и средства выхода в информационно-телекоммуникационную сеть «Интернет». Если хотя бы одна из этих функций не будет поддерживаться устройством – нужно ли будет получать судебное решение?

Выработка новых юридических подходов, применительно к обыску сотового телефона задержанного посредством судебных решений, бесспорно, помогает праву более оперативно реагировать на происходящие общественные изменения. При этом, суд, как известно, решает вопрос о законности того или иного действия и не нацелен на выработку какого-либо глубокого системного решения той или иной проблемы. Законодательные органы имеют больше средств для разрешения проблем, связанных с обеспечением сохранности персональных данных владельцев мобильных устройств, чем органы правосудия, наделенные возможностью формировать судебную практику лишь в контексте отдельных ситуаций.

С учетом ситуационного характера принятого решения, определенный интерес представляют рекомендации американских правоведов об ограничении полномочий полиции при обыске электронного устройства задержанного.

К примеру, некоторые американских юристы, включая судей, указывают на необходимость установления запрета на обыск телефона по любому преступлению, кроме как по тому, за совершение которого лицо было задержано [2, p. 22]. Иными словами, информация, не относящиеся к расследуемому деянию, даже при своей явной противоправности, должна процессуально игнорироваться лицом, производящим обыск сотового телефона. Те же данные, которые относятся к расследуемому событию, могут быть получены, как и ранее, без судебной санкции.

Вторая рекомендация предполагает установление так называемого критерия «открытого приложения», согласно которому полицейских может получать данные лишь из тех программ сотового телефона или смартфона, которые уже запущены. При этом, он не вправе открывать новые приложения [2, p. 28].

Еще одним способом решения обозначенной проблемы ведется установление ограниченного количества воздействий, которые сотрудник правоохранительного может произвести через интерфейс сотового телефона [2, p. 30]. Предлагается установить, что, к примеру, после пяти воздействий дальнейших поиск информации необходимо прекратить.

Некоторые правоведы предлагают также отделить информацию, хранящуюся в памяти самого устройства от данных, получаемых через доступ к информационно-телекоммуникационной сети «Интернет», и на основании этого уже определять какие данные подлежат исследованию, а какие – нет [2, p. 31].

Все предложенные варианты имеют свои достоинства и недостатки, однако само существование различных подходов по указанному вопросу демонстрирует одно – вопросы исследования содержания цифровых устройств обладают определенной спецификой, которая должна быть учтена при дальнейшем совершенствовании американского уголовно-процессуального права.

Данные выводы имеют ценность и для развития современного отечественного законодательства, поскольку граждане РФ также активно используют передовые информационные технологии не только в своей работе, но и в повседневной жизни, что предполагает хранение значительного числа сведений о личности в памяти портативных электронных устройств.

Вместе с тем, отечественная правовая доктрина в настоящее время не уделяет должного внимания проблеме исследования цифровых технологий. Те же работы, которые посвящены данному вопросу, акцентируют внимание на технических и криминалистических аспектах деятельности по сбору персональных данных в электронной форме, в то время как зарубежный опыт чаще всего увязывает подобные темы с такой важной правовой проблемой как обеспечение прав граждан на тайну личной жизни [5, p. 52].

Учитывая изложенное, ознакомление с юридической доктриной и судебной практикой США по данному вопросу представляется полезным и для российского юриста.

Библиография:

1. Бернам У. Правовая система США. М. 2006. – 1216 с.
2. Adam M.G. The iphone meets the fourth amendment. // UCLA Law Review. 2008. Vol. 27. – P. 27-58.
3. Bailie M.V., Hagen E., Judish N., Marshall J.H. Searching and seizing computers and obtaining electronic evidence in criminal investigations. Washington, 2009. – 287 p.
4. Brown P. Searches of cell phones incident to arrest: overview of the law as it stands and a new path forward. // Harvard Journal of Law and Technology. 2014. Vol. 27. – P. 563-586.
5. Chang R.M. Why the plain view doctrine should not apply to digital evidence // Journal of Trial and Appellate Advocacy. Vol. XII. 2010. – P. 31-67.
6. Nelson J.C. United states v. Robinson, 414 U.S. 218 (1973). // Akron Law Review. 1974. Vol. 7:3. – P. 499-507.
7. Pincus A. Evolving technology and fourth amendment: the implication of Riley v. California. // Cato Supreme Court Review. 2014. – P. 307-336.
8. Riley v. California, 573 U.S. 2014. – 28 p.
9. Starbuck J.L. Redefining searches incident to arrest: Gant's Effect on Chimel. // Penn State Law Review. 2012. Vol. 116:4. – P. 1253-1280.
10. U.S. Supreme Court's Cellphone Ruling Is a Major Victory for Privacy. // Newsweek. [Electronic resource]. URL: (last access 28.11.2014).

References (transliterated):

1. Bernam U. Pravovaya sistema SShA. M. 2006. – 1216 s.
2. Adam M.G. The iphone meets the fourth amendment. // UCLA Law Review. 2008. Vol. 27. – P. 27-58.
3. Bailie M.V., Hagen E., Judish N., Marshall J.H. Searching and seizing computers and obtaining electronic evidence in criminal investigations. Washington, 2009. – 287 r.
4. Brown P. Searches of cell phones incident to arrest: overview of the law as it stands and a new path forward. // Harvard Journal of Law and Technology. 2014. Vol. 27. – P. 563-586.

DOI: 10.7256/1811-9018.2014.12.13846
При цитировании этой статьи сноска на doi обязательна

5. Chang R.M. Why the plain view doctrine should not apply to digital evidence // Journal of Trial and Appellate Advocacy. Vol. XII. 2010. – P. 31-67.
6. Nelson J.C. United states v. Robinson, 414 U.S. 218 (1973). // Akron Law Review. 1974. Vol. 7:3. – P. 499-507.
7. Pincus A. Evolving technology and fourth amendment: the implication of Riley v. California. // Cato Supreme Court Review. 2014. – P. 307-336.
8. Riley v. California, 573 U.S. 2014. – 28 p.
9. Starbuck J.L. Redefining searches incident to arrest: Gant's Effect on Chimel. // Penn State Law Review. 2012. Vol. 116:4. – P. 1253-1280.