Министерство образования и науки Российской Федерации
Федеральное государственное Бюджетное образовательное учреждение высшего образования
«Уральский государственный юридический университет»

ТРАНСФОРМАЦИЯ ПРАВА В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Материалы I Всероссийского научно-практического форума молодых ученых и студентов
(Екатеринбург, 21 марта 2019 года)

Екатеринбург 2019

УДК 34(063)
ББК 67я431
П 684

Печатается по постановлению ученого совета
Института прокуратуры
Уральского государственного юридического университета

Ответственный редактор

Доктор юридических наук, профессор О.А. Пучков

П 68 Трансформация права в информационном обществе: материалы I Всероссийского научно-практического форума молодых ученых и студентов

(Екатеринбург, 21 марта 2019 года) / отв. ред. О.А. Пучков. – Екатеринбург:

ISBN 978-5-7845-0554-5

Сборник включает в себя тексты выступлений и докладов, посвященных организационноправовым проблемам развития государства и права, правовой науки, спорным вопросам правоприменения.

Студентам, аспирантам и преподавателям юридических вузов.

Материалы печатаются в авторской редакции

УДК 34 (063)
ББК 67я431

ISBN 978-5-7845-0554-5

ilyahl@icloud.com
alina_golysheva@mail.ru

RESPONSIBILITY FOR ACTIONS ON SOCIAL NETWORKS

Abstract: The article elaborates on criminal responsibility for actions in the social networks in the Internet. In particular, the author analyzes the concept of "terrorism justification", considers responsibility for separate actions, makes a conclusion regarding the need of establishing all circumstances of each fact, including existence of express malice and subject of a crime, which are necessary for bringing to responsibility.
Key words: criminal liability; social networks; extremism; justification of terrorism; information spreading.

УДК 343.3.7

Эткина Алиса Дмитриевна
Российский государственный университет правосудия
Россия, Москва
Aliceetkina@gmail.com

АКТУАЛЬНЫЕ ВОПРОСЫ ОПРЕДЕЛЕНИЯ МЕСТА СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЯ

Аннотация: Данная статья посвящена вопросам определения места совершения киберпреступления. Автором рассматриваются вопросы, возникающие при совершении такого деяния с территории одного государства, причиняя вред интересам второго, гражданином третьего государства.
Ключевые слова: место совершения преступления; время совершения преступления; киберпреступление.

В настоящее время множество преступлений совершаются с помощью информационно-телекоммуникационых сетей. Злоумышленники активно используют современные технологии при совершении преступления. Как следствие, законодатель вводит уголовную ответственность за новые киберпреступления, однако не разрешает при этом вопрос о месте совершения киберпреступления и связанные с этим аспекты уголовной юрисдикции. Данная проблема актуальна не только для целей уголовного судопроизводства (с точки зрения территориальной подследственности и подсудности киберпреступлений), но и для определения действующего уголовного закона при трансграничном характере таких преступлений, так как государство, на чьей территории совершено преступление, имеет право на применение своего уголовного законодательства к нарушителю. Все чаще такие преступления совершаются следующим образом: на территории государства «А» гражданин государства «Б»

совершает киберпреступление, которое посягает на интересы государства «В» (например, похищает денежные средства с банковского счета гражданина или организации государства «В»). В такой ситуации все три государства имеют право на применение своего законодательства (государство «А» по территориальному принципу; государство «Б» по принципу гражданства; государство «В» по реальному принципу). При этом важно то, что в соответствии с Конвенцией о преступности в сфере компьютерной информации от 23.11.2001 г. [1] в данной ситуации применимое право зависит только от договора между странами. Необходимо напомнить, что Россия отозвала свою подпись к данной Конвенции, поэтому даже это правило для нее не обязательно. При этом следует иметь в виду, что санкции за одно и то же деяние в уголовном законе разных государств могут существенно различаться, что не всегда соответствует принципу справедливости.

Ряд авторов полагают, что местом киберпреступления является само киберпространство (например, А.К. Киселев, а также М.С. Дашян) [2, с. 81]. Подобная позиция является очень удобной с точки зрения доказывания, сразу снимается необходимость привязки серверов, IP и MAC-адресов к конкретным географическим координатам. Однако уголовной ответственности подлежит человек, который находится в реальном мире, а не его компьютер или аккаунт. Необходимо определить место действия именно человека. Также важным аспектом является понимание сущности самого киберпространства. Первое его легальное определение дал Верховный Суда США, который определяет киберпространство как уникальную среду, не расположенную в географическом пространстве, но доступную каждому в любой точке мира посредством доступа в Интернет [3]. С данным определением трудно согласиться, так как данная «уникальная среда» создается из конкретных объектов реального мира, которые находятся в конкретных географических координатах. Поэтому, на наш взгляд, более корректным определением является, то, которое содержится в Концепции Стратегии кибербезопасности Российской Федерации. В ней закреплено, что киберпространство – это сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства) [4]. Данное определение представляется нам достаточно емким и отражающим сущность киберпространства. Такое понимание киберпространства позволяет произвести соотношение действий человека, который совершает киберпреступление, и географических координат. Условно это выглядит следующим образом: человек совершает ввод данных с компьютера, который вышел в сеть в точке «А», с компьютера поступил запрос на сервер в точке «Б» (там могут быть похищены денежные средства или может быть совершено иное преступление). Далее информация с сервера точки «Б» может поступить в одну из территориальных организаций (точка «В»), которая еще ранее дала поручение операционному центру (который находится в точке

«Б») на обработку транзакций. Как правило, именно точка В находится в более тесных правовых отношениях с потерпевшим. При этом местоположение потерпевшего в данном случае не влечет никаких уголовно-правовых последствий.

В.А. Тирранен считает, что место совершения киберпреступления необходимо определить как виртуальное пространство, находящееся вне территории любого государства [5, с. 410]. На наш взгляд, понятие виртуального пространства является слишком широким для целей уголовного права. Под виртуальным принято понимать все, что может представить человек, это его мыслительная деятельность, направленная на представление чего-то (не обязательно реалистичного). Как следствие, это может привести к поднятию вопроса об уголовной ответственности за мысли (т.е. стадии обнаружения умысла на совершение преступления), что является недопустимым.

М.А. Федотов пишет, что при сложившихся обстоятельствах необходимо формирование новой отрасли права – права киберпространства, так как современные инструменты правового регулирования (как на национальном, так и на наднациональном уровне) не обладают достаточной эффективностью для упорядочения данных взаимоотношений. Автор подчеркивает особую важность таких способов контроля в информационно-телекоммуникационном пространстве, как саморегулирование и программный код [6, с. 164]. Так как киберпространство не принадлежит ни одному государству, то если местом преступления является само киберпространство, то можно предположить, что там должны действовать свои законы и суды, что на данном этапе невозможно. Определенные подвижки в данном вопросе сделал Китай, создав специализированный онлайн суд, в юрисдикции которого находятся только киберпреступления [7]. Однако в настоящее время данная мера реализована только в одном государстве, а для того чтобы признать киберпространство местом преступления, необходимы аналогичные меры всех государств, поэтому мы не можем сейчас рассматривать киберпространство как место преступления. К тому же, следует помнить, что лицо, совершившее киберпреступление, находится в реальном мире, и последствия (не только те, которые входят в конструкцию состава преступлении, но и более отдаленные) проявляются также не только в киберпространстве, но и в реальности.

Иначе говоря, на наш взгляд, киберпространство (в понимании «уникального пространства», «альтернативной реальности» и пр.) не может являться местом совершения преступления. Однако это не решает проблему, а только сужает круг поиска ответа на поставленный вопрос. Далее необходимо понять, что является местом совершения киберпреступления: сервер, на который была совершена атака (например, в результате такой атаки были похищены денежные средства с банковского счета), место наступления общественно опасных последствий (например, смерть человека) или место ввода компьютерных данных.

Также особый интерес представляет абз. 2 п. 5 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам

о мошенничестве, присвоении и растрате» [8], в котором указано, что если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Иначе говоря, момент окончания преступления был перенесен к моменту изменения данных на сервере процессингового центра банка. Как следствие, место наступления последствий уже не может признаваться местом совершения киберпреступления. К тому же, признание местом совершения такого преступления места наступления общественно опасных последствий вызвало бы множество вопросов применительно к преступлениям с формальным составом, например, незаконному изготовлению и обороту порнографических материалов или предметов (ст. 242 Уголовного кодекса Российской Федерации (далее – УК РФ)).

Важно понимать, что при совершении преступления в сфере компьютерной информации может быть несколько мест происшествия: 1 – рабочее место, рабочая станция – место обработки информации, ставшей предметом преступного посягательства; 2 – удаленное место управления сетевыми ресурсами, хранения или резервирования информации, в частности, сервер, ставший предметом преступного посягательства или сохранивший свидетельства о нем и о работе системы за определенный период, стример; 3 – место использования технических средств для неправомерного доступа к компьютерной информации, нарушение работы ЭВМ, системы ЭВМ или их сети; 4 – место наступления вредных последствий, место хранения информации, полученной в результате неправомерного доступа к данным, содержащимся на машинных носителях или в ЭВМ [9, с. 7]. При этом необходимо помнить, что место преступления и место происшествия могут не совпадать. Место происшествия – это любой участок, в пределах которого обнаружены следы преступления, хотя само преступление могло быть совершено в другом месте.

М.А Простосердов полагает, что местом совершения деяния является место, где виновный совершил ввод компьютерных данных, то есть это место доступа в киберпространство [10, с. 58]. С данным утверждением трудно не согласиться, так как преступление всегда выражается в форме деяния в виде действия. В данном случае действие совершается в точке ввода компьютерной информации и точке выхода в сеть, а модификация данных на сервере является уже следствием ввода таких данных. При этом необходимо соотнести место совершения киберпреступления и время его совершения. УК РФ содержит легальное определение времени совершения преступления, в отличие от определения места совершения преступления. В соответствии с ч. 2 ст. 9 УК РФ под временем совершения преступления понимается время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий.

Таким образом, местом совершения киберпреступления необходимо признать место ввода компьютерной информации и выхода в сеть, так как именно в этот момент совершается преступное деяние.

Список литературы

1. Конвенция о преступности в сфере компьютерной информации от 23.11.2001 г (ETS № 185). Документ опубликован не был. Текст документа доступен в СПС КонсультантПлюс.
2. См.: Киселев А.К. Киберпреступность – взгляд из Европы // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). С. 310; Дашян М.С. Право информационных магистралей: вопрос правового регулирования в сети «Интернет». М., 2007. С. 81.
3. Reno vs. ACLU, 117 S.Ct. 2329 (1997) (casebook at 932-53) [Электронный ресурс] // Режим доступа: www.ciec.org/SC_appeal/opinion.shtml. (Дата обращения: 04.03.2019).
4. Проект Концепции Стратегии кибербезопасности Российской Федерации [Электронный ресурс] // Электронный документ. Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a7 (Дата обращения: 04.03.2019).
5. Тирранен В.А. Тенденции развития уголовного законодательства в сфере борьбы с киберпреступностью // Уголовное право: стратегия развития в XXI веке. Материалы XII Международной научно-практической конференции (29-30 января 2015 г.). М., 2015. С. 410.
6. Федотов М.А. Конституционные ответы на вызовы киберпространства // Lex Russica. 2016. № 3. С. 164.
7. В Китае начал работу первый в стране интернет-суд. Комсомольская правда [Электронный ресурс] // Режим доступа: https://www.kp.ru/online/news/2841392/ (Дата обращения: 04.03.2019).
8. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. 2017. 11 декабря.
9. Гаврилов М.В., Иванов А.Н. Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации: учебное пособие. Саратов, 2004. С. 7.
10. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве: монография. М., 2017. С. 58.

Etkina Alise
Russian state university of justice
Russia, Moscow
Aliceetkina@gmail.com

CURRENT ISSUES OF DETERMINING THE PLACE OF THE PERFORMANCE OF CYBER CRIMES