УДК 343.232

В статье затронуты основные аспекты проблемы трансграничности применительно к ее влиянию на уголовно-правовое регулирование отношений в сфере кибертехнологий. Автором отмечено, что киберпреступления обычно обладают транснациональным характером с учетом особенностей их проявлений на территории того или иного государства. Следовательно, под транснационализацией киберпреступной деятельности понимается выход за пределы единой территории, на которой проживают граждане одного государства. В условиях глобализации трансграничные свойства киберпреступности характеризуются постоянной трансформацией их традиционных форм, усложнением и политизацией преступных проявлений исходя из того, что некоторые государства используют транснациональные организованные преступные группировки в собственных интересах. Кроме того, к настоящему времени у транснациональной организованной киберпреступности сложились свои характерные только для нее методы преступной деятельности и векторы активности ее членов.

Ключевые слова: уголовное право, киберпреступность, кибертехнологии, трансграничность, правовое регулирование, нормативный акт, национальное законодательство.

This article covers the main aspects of the problem of transboundary issues in relation to its impact on the criminal law regulation of the sphere of cybertechnologies. The author noted that cybercrimes usually have a transnational character, taking into account the characteristics of their manifestations in the territory of a particular state. Consequently, the transnationalization of cybercrime activities is understood as going beyond the territorial limits of a single state territory where citizens of one state reside. The article states that in the context of globalization, the transboundary properties of cybercrime are characterized by a constant transformation of their traditional forms, constant complication and politicization of criminal manifestations on the basis that some states use transnational organized criminal groups in their own interests. The author states that so far transnational organized cybercrime had its own, characteristic only for it, methods of criminal activity and vectors of activity of its members.

Keywords: criminal law, cybercrime, cyber technologies, cross-border, legal regulation, normative act, national legislation.

Д. В. Пучков

Уральский государственный юридический университет
E-mail: puchkov@puchkovpartners.ru

Проблема трансграничности в уголовно-правовом регулировании отношений в сфере кибертехнологий

Научная статья

D. V. Puchkov

Ural State Law University

The problem of cross-border in the criminal-legal regulation of the sphere of implementation of cyber technologies

Scientific article

Начало XXI в. ознаменовалось расширением масштабов и влияния транснациональной организованной преступности как реальной угрозы безопасности большинства государств мира [1, с. 24–45]. В свою очередь, осознание опасности транснациональной организованной преступности как глобального явления и адекватное реагирование на нее стали активизироваться только в конце XX в. Несмотря на предпринимаемые усилия ученых описать и систематизировать информацию по транснациональной преступности, даже в настоящее время отсутствуют всеобъемлющие параметры оценки данного явления. В основном, на доктринальном уровне изучение транснациональной преступности сводится к дискуссиям по поводу самого понятия данного явления и его актуализации на национальном уровне [2, с. 35].

Широкое использование кибернетических технологий в современном мире ускоряет их трансформацию и придает им новое качественное состояние, ввиду чего и происходит технологическая модернизация ключевых сфер жизнедеятельности

современного государства. Процесс трансформации возможно описать с использованием такого философского концепта, как «*трансгрессия*», под которым понимается «смещение и стирание границ – границ между вещами и между ценностями. Она предполагает выход предмета за собственные границы», а также «…являет собой невозможный (в данной системе отсчета) выход за пределы, прорыв вовне того, что принадлежит наличному» [3, с. 665].

Одной из основных особенностей акта трансгрессии выступает нарушение линейности определенного процесса. Именно трансгрессия позволяет выявить степень радикальности изменений такого феномена, как кибертехнологии, посредством которых общество может трансформироваться в сторону развития духовной, ценностно-мотивационной сфер человеческой деятельности. Этот вопрос приобретает особую актуальность ввиду все чаще звучащего мнения о вторичности задачи обеспечения элементарной жизнедеятельности общества по сравнению с необходимостью установления стратегического контроля над общественным сознанием с перспективой получения практически безграничной власти над социумом.

Проблема усугубляется тем, что глобализация уже сама по себе влияет на взаимозависимость территориального определения государственных границ, государственного суверенитета и эффективность национальной правовой системы. Как подчеркивает В. И. Червонюк, «действие права означает, что феномен «право» самим фактом своего существования создает правовое пространство, в котором протекает жизнедеятельность индивидов, общностей людей, общества в целом» [4, с. 406]. Это со всей очевидностью предполагает *технико-юридическую универсализацию, стандартизацию и гармонизацию национальных правовых систем*. В этом контексте особую значимость приобретает проблема киберпреступлений, которые в своей массе (от 30 до 70 %) обладают транснациональным характером, причем противодействие этим преступлениям сопряжено с проблемами транснациональных расследований, юрисдикции, национального суверенитета, что обусловливает необходимость в экстерриториальных доказательствах и потребность в создании устойчивой системы международного сотрудничества.

Киберпреступления обычно носят транснациональный характер при наличии фактов проявления на территории того или иного государства какого-либо признака международного характера или масштабных последствий этого преступления либо при совершении части данного киберпреступления на территории иной страны. Следовательно, под транснационализацией киберпреступной деятельности понимается выход за пределы единой государственной территории, на которой проживают граждане одного государства. Такая ситуация в условиях глобализации предстает как один из высших уровней в процессе «криминальной эволюции» [5, с. 5].

В данном случае территориальная привязка применима как к элементам, так и последствиям преступных деяний, а также учитывает место нахождения информационно-коммуникативных систем или данных, которые используются для совершения киберпреступления. При возникновении тех или иных юрисдикционных конфликтов их разрешение обычно происходит с использованием специальных консультаций между государствами, которые могут обладать как официальным, так и неофициальным статусом. Этим во многом объясняется отсутствие стремления государств обеспечить дополнительную форму юрисдикции, касающуюся виртуальной категории «киберпространство».

Усиление интереса к проблеме трансграничности во многом обусловлено противоречиями между регионализацией и глобализацией. По своей сути и понятие «трансграничный», и понятие «транснациональный» выступают как собирательные в отношении всех преступлений, которые совершаются на конкретной территории или затрагивают интересы более чем одного государства. В этой связи следует опираться на традиционную классификацию преступлений в рамках международного уголовного права. Так, например, понятие «транснациональное преступление» раскрывается в Конвенции ООН против транснациональной организованной преступности (2000 г.) [6]. Тем не менее представленное в этой Конвенции определение содержит достаточно широкое толкование указанного термина в силу того, что в него включен ряд признаков:

- совершение преступления более чем в одном государстве;

- совершение преступления в одном государстве при условиях его подготовки, планировании, руководстве или контроле в ином государстве;

- преступление совершено в одном государстве, но в его совершении принимала участие организованная преступная группа, осуществляющая

преступную деятельность за пределами этого государства;

- преступление совершено в одном государстве, но его значительные последствия нашли свое отражение в другом. При этом преступления международного характера часто называются конвенционными, так как их определение и регулирование осуществляется в международных конвенциях.

Анализируемая Конвенция ООН против транснациональной организованной преступности задает четкие параметры формирования и развития правовых основ законодательства в этой сфере на национальном уровне, а также определяет основания международного сотрудничества применительно к единой политике противодействия существующим видам организованной преступности, характеризующейся транснациональным характером.

Необходимо указать на различие в возможном использовании терминов «международный» и «трансграничный». В первом случае использование термина «международный» может быть связано с регулированием отношений, построенных на международно-правовых актах и определяющих легальные отношения. Во втором случае при использовании закрепленного в Конвенции ООН против транснациональной организованной преступности термина «транснациональный» должна быть раскрыта специфика самой организованной преступной деятельности представителей иностранных государств или лиц без гражданства. При этом следует учитывать и то, что в настоящее время, помимо термина «транснациональный» [7, с. 1339], часто применяется и термин «трансграничный». Законодательство государств в рамках СНГ оперирует двумя этими терминами. Но, несмотря на то что общекоренное значение данных терминов их объединяет, содержание других корней, как справедливо подмечено в науке, не идентично по смыслу [8, с. 99].

Трансграничная преступность как специфический вид преступности в целом представляет собой многокачественное и многомерное понятие, предполагающее различные подходы в его исследовании. Так, рост количества трансграничных преступлений способствовал возникновению в процессуальном законодательстве ЕС категории «трансграничный потерпевший», определение которой раскрыто в Директиве ЕС № 2004/80/ЕС от 29 апреля 2004 г. «О возмещении ущерба жертвам преступности» [9]. В соответствии с положениями данной директивы, под трансграничным потерпевшим понимается «гражданин Европейского Союза, который стал жертвой преступления в государстве-члене, отличном от того, где он постоянно проживает» [9].

Полагаем, что при использовании таких понятий, как «транснациональный» или «трансграничный», следует учитывать их различия по смыслу, которое основано «в первом случае на принадлежности участников организованных преступных формирований к гражданству государства (в отдельных случаях, государств), то есть на личности правонарушителя, во втором – на месте совершения преступления» [10, с. 233]. Касательно большинства подобных преступлений можно говорить о существовании различных международных соглашений и конвенций, благодаря которым у государств могут возникать определенные обязательства, связанные с пресечением преступлений или привлечением к уголовной ответственности, а также об осуществлении иных форм сотрудничества.

По ряду признаков трансграничная киберпреступность имеет определенное совпадение с общими критериями организованной преступности, и особенно с признаками транснациональных преступных организаций. Предложения, связанные с определением сущности транснациональной организованной преступности, были рассмотрены еще в 1988 г. на международном симпозиуме в Сант-Клауде. Как результат обсуждения участниками конференции из 46 государств – членов Интерпола было достигнуто соглашение о принятии за основу следующего понятия «транснациональная организованная преступность» – это «любое участие или организация группы людей, которые непрерывно практикуют преступную деятельность и чья главная цель – делать прибыль везде, безотносительно к национальным границам» [5, с. 8]. Следовательно, основа понимания сущности трансграничной киберпреступности находится в максимальной зависимости от специфики преступной деятельности, определяющей существование транснациональной преступной организации.

Исходя из общепринятых трактовок, существующих на доктринальном уровне, следует отметить, что преступления трансграничного характера – это деяния, которые, во-первых, предусмотрены международными соглашениями. Во-вторых, их объектом являются нормальные отношения между различными государствами. В-третьих, они причиняют определенный ущерб позитивному межгосударственному сотрудничеству в той или иной области межгосударственных отношений и подле-

жат наказанию исходя из положений уголовного закона на национальном уровне. При этом в международном праве существуют некоторые обстоятельства для определения юрисдикции применительно к подобного рода деяниям, включая выбор юрисдикции на основе принципа территориальности и юрисдикции, в основу которой положено гражданство.

Вместе с тем к настоящему времени не выработано единой классификации международных преступлений, которые в своем большинстве обладают универсальной юрисдикцией, что предполагает возможность осуществления конкретных мероприятий специальными органами определенного государства. Речь идет о мерах по пресечению преступной деятельности или привлечению к уголовной ответственности в рамках национального законодательства в случае, если указанное государство есть участник международного договора, регламентирующего ответственность за это преступление.

Ряд правовых оснований вытекает из актов международного характера, связанных с предупреждением киберпреступности, тем не менее экспертным сообществом признается недостаточность существующей правовой базы для криминализации и целенаправленного преследования экстерриториальных киберпреступлений. Определение данного ключевого признака организованной преступности, действующей на транснациональном уровне, способно указать на границы между организованным преступным формированием, состоящим из граждан одного государства, и транснациональным организованным преступным формированием, в состав которого входят граждане различных государств. Поэтому при исследовании понятия и сущности транснациональной организованной киберпреступности невозможно учитывать только характеристику собственно преступной деятельности. Особое значение при этом имеет и характеристика самих субъектов этой деятельности. Так, при рассмотрении организованной транснациональной киберпреступности кроме такого признака, как «совершение преступления в иностранной юрисдикции», следует учитывать и непрерывность осуществления преступных деяний, масштаб их распространения в нескольких юрисдикциях, дублирование, а порой и прикрытие преступной деятельности под осуществление легальных операций международного характера.

В настоящее время сеть Интернет уже используется организованными преступными сообществами в качестве основного средства и среды совершения общеуголовных преступлений: краж, вымогательств, мошенничеств и т. д. Но масштаб киберпреступлений проявляется в деятельности организованных преступных группировок и посредством вмешательства в сетевые банковские операции, связанные с дистанционным банковским обслуживанием. Подобные методы использования информационно-коммуникативных сетей есть не только следствие, но и фактор мировой экономической интеграции. Ее основу как раз и составляет оказание финансовых услуг и применение электронных форм торговли. В частности, следствием глобального развития информационно-коммуникативной сети Интернет стало совершение на транснациональном уровне киберпреступлений в сфере обращения электронных денег, взаимодействия виртуальных магазинов, банков и бирж.

Особенностью совершения подобного рода преступлений является низкий уровень возможностей их выявления, определения масштабов ущерба и даже потерпевших. При наличии огромного количества электронных транзакций, имеющих место в рамках электронного оборота финансовых ресурсов, требуется достаточно значительные временные затраты, сопровождающиеся также привлечением специалистов высокого уровня для выявления и расследования таких преступлений. Другой особенностью этих преступлений является привлечение к преступной деятельности сторонних лиц, среди которых особое место занимают собственно разработчики используемого финансовыми организациями программного обеспечения и хакеры высокого уровня. Подобное расширение масштабов преступной деятельности часто находится на грани вмешательства в финансовую деятельность как на национальном, так и на международном уровне, что рассматривается уже как потенциальная угроза национальной безопасности государства и мирового сообщества в целом.

Важно отметить, что в условиях глобализации трансграничные свойства киберпреступности характеризуются постоянными видоизменениями их традиционных форм, постоянным усложнением и политизацией преступных проявлений, особенно если принять во внимание тот факт, что некоторые государства используют транснациональные организованные преступные группировки в собственных интересах. Помимо этого, к особенностям взаимодействия между киберпреступниками следует отнести достаточно малое количество

непосредственных контактов. Как правило, они общаются в виртуальном пространстве и по анонимным каналам, предполагающим обеспечение максимальной конспирации личностей каждого из них [11, с. 54–56]. В целом анонимность в этой среде является одним из условий не только нераскрытия личности преступника, но и обеспечения его активной жизнедеятельности. Использование так называемого «темного Интернета» как раз и позволяет минимизировать риски в системе взаимодействия преступников между собой.

Таким образом, возможно говорить, что транснациональной организованной киберпреступности присущи следующие признаки:

- существование преступных группировок с различным уровнем организованности, в состав которых входят граждане двух и более государств;
- использование насильственного или коррупционного механизмов при осуществлении преступной деятельности и достижении своих целей;
- применение киберпреступных видов деятельности не только в незаконных, но и в легальных сферах;
- планирование, совершение или нахождение последствий киберпреступной деятельности в юрисдикции двух или более государств;
- активное использование различного вида транснациональных взаимосвязей при осуществлении организованной преступной деятельности.

Ссылки

1. Долгова А. И. Преступность в России начала XXI века и реагирование на нее. М., 2004. 244 с.

2. Сухаренко А. Н. Транснациональные аспекты деятельности российской организованной преступности // Организованная преступность, терроризм, коррупция в их проявлениях и борьба с ними. М., 2005. С. 33–36.

3. Новейший философский словарь. Постмодернизм / ред. А. А. Грицанов. Мн., 2007. 816 с.

4. Червонюк В. И. Теория государства и права: учебник. М., 2009. 457 с.

5. Воронин Ю. А. Транснациональная организованная преступность. Екатеринбург, 1997. 205 с.

6. Конвенция ООН против транснациональной организованной преступности. URL: http://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml (дата обращения:11.01.2019 г.).

7. Большой толковый словарь русского языка / сост и гл. ред. С. А. Кузнецов. СПб., 2000. 1536 с.

8. Щеблыкина И. В. Организованная преступность транснационального, трансграничного характера и криминологическая ситуация в пограничном пространстве России // Совершенствование борьбы с организованной преступностью, коррупцией и экстремизмом / под ред. А. И. Долговой. М., 2008. С. 98–105.

9. Директива ЕС № 2004/80/ЕС от 29 апреля 2004 г. «О возмещении ущерба жертвам преступности» // Official Journal of the European Union. 2004. L. 261. URL: http://eur-lex.europa.eu/oj/direct-access.html (дата обращения: 11.01.2019 г.).

10. Щеблыкина И. В. Транснациональная организованная преступность в пограничной сфере Российской Федерации в условиях глобализации преступности // Научные основы уголовного права и процессы глобализации: Материалы V Российского Конгресса уголовного права (27–28 мая 2010 г.). М., 2010. С. 232–234.

11. Хижняк Д. С. Информационные модели транснациональной криминальной деятельности. М., 2018. 248 с.