



*А.К. Расулев, доктор юрид. наук, профессор
Академия МВД Республики Узбекистан*

НЕКОТОРЫЕ ВОПРОСЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

Эффективное решение проблемы борьбы с информационными преступлениями требует согласованных международных действий и сотрудничества. В процессе проведения расследований правоохранительные органы различных государств должны сотрудничать между собой, предоставляя потенциально полезную информацию непосредственно органам другого государства. Вместе с тем в зависимости от отношений между заинтересованными государствами, характера соответствующей информации и других факторов может также возникать потребность в разработке полномочий и процедур в международном соглашении [7, с. 306].

Итак, в чем можно увидеть основные проблемы международного сотрудничества по уголовным делам, в частности по делам о преступлениях в сфере информационных технологий и безопасности?

Во-первых, наступил момент истины, когда мировое сообщество, национальные институты по борьбе и противодействию преступлениям в сфере информационных технологий и безопасности должны провести критический анализ и пересмотреть свои подходы, мировоззрения по вопросам унификации и гармонизации норм уголовного законодательства всех стран. Это связано с тем, что в глобальном информационном пространстве уголовно-правовая политика каждого государства оказывает непосредственное влияние на криминогенную характеристику уровня информационной преступности в целом. К сожалению, в глобальных сетях присутствуют национальные сегменты, где не криминализованы определенные преступные действия, что, в свою очередь, позволяет преступникам активно осваивать эти «островки беззакония и хаоса».

Несмотря на то что проходит второе десятилетие XXI в., до сих пор есть государства, в которых практически отсутствуют законы, устанавливающие ответственность за все существующие на практике виды информационных преступлений. Так, по данным проведенного под эгидой ООН еще в 2002 г. исследования фирмы McConnell International, в уголовные кодексы 33 из 52 государств не внесены необходимые изменения, направленные на борьбу с киберпреступностью [3, с. 18]. Несмотря на то что сегодня эта картина существенно меняется, уголов-

ное законодательство ряда развивающихся стран, в частности Анголы, Багамских островов и Уганды, не содержит статей, предусматривающих ответственность за преступления в сфере информационных технологий [8, 9].

Общее восприятие киберпреступлений как преступлений, имеющих транснациональный характер, требует тщательного анализа. Одной из отправных точек является подход Конвенции ООН против организованной преступности, который предусматривает, что преступление имеет «транснациональный характер», если (i) оно совершено в более чем одном государстве, (ii) оно совершено в одном государстве, но существенная часть его подготовки, планирования, руководства или контроля прошли в другом государстве, (iii) оно совершено в одном государстве, но при участии организованной группы, которая осуществляет преступную деятельность в более чем одном государстве, или (iv) оно совершено в одном государстве, но имеет существенные последствия на территории другого государства [2]. Ярким подтверждением данной позиции является статья 11 УК Республики Узбекистан (действие Кодекса в отношении лиц, совершивших преступления на территории Узбекистана).

Во-вторых, с учетом дальнейшего и неизбежного роста глобализации возник вопрос о необходимости рассмотрения проблемы по разработке глобального общеобязательного международного акта, предусматривающего общие принципы борьбы с информационными преступлениями, вопросы гражданской и уголовной ответственности, перечень уголовно наказуемых деяний, конкретные механизмы международного сотрудничества в области противодействия информационным преступлениям и повышения квалификации сотрудников правоохранительных органов, обмена данными и судопроизводства.

За последние годы вопросы противодействия трансграничным преступлениям, в частности киберпреступности, на региональном уровне обсуждаются регулярно и системно. В частности, можно отметить усилия авторитетной региональной Шанхайской организации сотрудничества (ШОС), под эгидой которой в июне 2017 г. в городе Ханты-Ман-

сийске состоялась 1-я Международная конференция по информационной безопасности с участием стран БРИКС (BRICS – сокращение от Brazil, Russia, India, China, South Africa), ШОС и Организации Договора о коллективной безопасности (ОДКБ). В работе конференции приняли участие представители Армении, Беларуси, Бразилии, Вьетнама, Казахстана, Малайзии, РФ и ЮАР [11]. Кроме того, 28-30 ноября 2017 г. на 15 заседании генеральных прокуроров – членов ШОС в Санкт-Петербурге были обсуждены вопросы консолидации усилий по противодействию новым вызовам и угрозам, в т.ч. преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий [12].

Кроме того, в Стратегии развития ШОС до 2025 г. особое внимание уделяется вопросу дальнейшего поэтапного реагирования на данную проблематику. В документе отмечено, что ШОС будет интенсивно и настойчиво добиваться принятия в ООН «Правил поведения в области обеспечения международной информационной безопасности» и в дальнейшем на этой основе совместно с другими членами мирового сообщества работать над формированием единого международного регулирования сферы ИКТ, развивать сотрудничество в этом направлении, в т.ч. в повышении квалификации профильных специалистов государств-членов в рамках Стратегии развития ШОС до 2025 г. Отрицательным фактом является то, что активную позицию в инициировании указанных Правил занимает Узбекистан. Это еще раз подчеркивает высокую обеспокоенность правительства ростом количества преступлений в области информационных технологий, усилением вызовов и угроз в сфере обеспечения международной информационной безопасности.

В качестве одного из основных региональных документов, заложивших основы международно-правового сотрудничества в области борьбы с киберпреступностью, можно отметить Конвенцию Совета Европы о киберпреступности 2001 года [3].

Однако следует отметить, что на глобальном уровне заметных и эффективных правовых актов в исследуемой сфере до сих пор не принято. В качестве таковых можно указать лишь Меры по борьбе против преступлений, связанных с использованием компьютеров, принятые на одиннадцатом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями в Бангкоке 25 апреля 2005 г. [13], Глобальную программу кибербезопасности, утвержденную Международным союзом электросвязи в 2007 г. [10], Окинавскую Хартию глобального информационного общества, принятую 23 июля 2000 г. [6] и ряд других, носящих рекомендательный, декларативный характер. В настоящее время можно также отметить резолюцию № 57/239 Генеральной Ассамблеи ООН от 20 декабря 2002 г.,

где установлены элементы для создания глобальной культуры кибербезопасности.

В-третьих, по причине отсутствия или декларативности и неэффективности международных соглашений страны предпочитают и вынуждены заключать двусторонние соглашения по оказанию взаимной правовой помощи, которые имеют более взаимовыгодный, действенный и оперативный характер реализации договоренности.

В настоящее время существуют около 40 двусторонних соглашений Республики Узбекистан с зарубежными государствами по вопросам взаимной помощи по уголовным делам. Однако лишь с четырьмя государствами (Азербайджан, Молдова, Туркменистан, Кувейт) предусматривается сотрудничество в области информационной безопасности, с семью странами (Австрия, Кипр, Беларусь, Иран, Саудовская Аравия, ОАЭ, Вьетнам) имеются соглашения в области противодействия компьютерным преступлениям и киберпреступлениям. Во многом приоритет двусторонних соглашений связан с тем, что надгосударственный характер глобальных сетей часто приводит к возникновению юрисдикционных проблем по фактам совершаемых киберпреступлений. Возникновение множественных правовых коллизий обуславливается трансграничным характером совершаемых деяний.

Заключение двусторонних соглашений между странами вызвано тем, что по причине отсутствия глобального уголовно-правового акта между странами не достигнут консенсус по вопросу эквивалентности криминализации. Это связано с особенностями международного сотрудничества. В частности, запросы о сотрудничестве, как правило, предполагают соответствие ряду процессуальных и материальных требований законодательства запрашиваемого государства. Одним из ключевых требований является *принцип двойной уголовной ответственности*. Данный принцип требует, чтобы деяние, к которому относится запрос, считалось преступлением в соответствии с уголовным законодательством как запрашиваемого, так и запрашивающего государства [14].

Так, к примеру, в Конвенции Совета Европы о компьютерных преступлениях уточняется, что принцип двойной уголовной ответственности считается соблюденным «независимо от того, относят ли данное правонарушение законы Стороны к преступлениям той же категории или использует ли она для обозначения этого преступления ту же терминологию, что и запрашивающая Сторона», если «деяние, лежащее в основе преступления», в связи с которым запрашивается помощь, «является уголовным преступлением согласно ее законам» [1].

В-четвертых, актуальной проблемой остается отсутствие на глобальном уровне единого центра

(органа) по координации борьбы с информационными преступлениями.

В качестве примера можно привести положительный опыт ЕС. На европейском континенте, ушедшем далеко вперед в плане интеграции и сотрудничества стран, основы взаимной правовой помощи сопровождаются новой тенденцией к взаимному признанию, в т.ч. за счет развития *европейского ордера на арест, ордера на получение доказательств и предложений по «европейскому ордеру на производство следственных действий»*¹. Европейские правовые документы, в частности, направлены на «централизацию судебного производства в одном [государстве]» [4].

Также механизмы официального сотрудничества, как правило, требуют определения *«центрального органа»*, который отвечает за обработку входящих и исходящих запросов по обычной или дипломатической почте. Соглашение СНГ, например, требует, чтобы государства-участники определили «перечень компетентных органов» [5]. Согласно данному соглашению компетентными органами Республики Узбекистан являются Министерство внутренних дел (МВД), Служба государственной безопасности (СГБ), государственный таможенный комитет (ГТК) и Генеральная прокуратура.

С учетом изложенного, а также проведенного анализа международных соглашений и нормативно-правовых актов зарубежных стран, не устанавливающих конкретных механизмов и не носящих концептуальный характер, различных противоречивых

позиций государств, можно прийти к мнению, что на сегодняшний день отсутствует единый консолидированный подход к решению проблемы. Эффективность международного сотрудничества зависит не только от усилий самих государств, но и от качества и действенности международных актов. Отсутствие действенных механизмов в рамках одного комплексного международного документа препятствует налаживанию эффективного международного сотрудничества.

Таким образом, одним из условий создания эффективной системы международной информационной безопасности является разработка и принятие современного, универсального международного правового акта, обеспечивающего адекватную защиту от новых угроз, при этом учитывающего национальный суверенитет государств в отличие от устаревшей европейской конвенции по киберпреступности. Заключение универсального международного договора о борьбе с информационными преступлениями, который учитывал бы накопившийся опыт международных соглашений в данной области и особенности национального законодательства стран-участниц, – довольно сложная и трудоемкая задача. Таким универсальным регулятором могла бы стать отдельная Конвенция ООН по борьбе с киберпреступлениями и обеспечению глобальной информационной безопасности, которая на международном уровне помогла бы комплексно и системно противодействовать киберпреступности и кибертерроризму, а также бороться с ними.

Литература

1. Будапештская конвенция по киберпреступлениям от 23 августа 2001 г. URL: www.mvd.gov.by (дата обращения: 25.02.2020).
2. Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 г. URL: www.un.org/ru/ (дата обращения: 25.02.2020).
3. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. М.: Норма, 2004. 80 с.
4. Рамочное решение Европейского парламента и Совета ЕС об атаках на информационные системы. URL: <http://docs.pravo.ru/document/view/22239321/21630736/> (дата обращения: 25.02.2020).
5. Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступностью // Сборник международных договоров Республики Узбекистан. 2010. № 1-4.
6. Старостина Е.В., Фролов Д.Б. Защита от компьютерных преступлений и кибертерроризма. Вопросы и ответы. URL: <http://kursak.net/kiberterrorizm-i-osobennosti-ego-proyavleniya/> (дата обращения: 25.02.2020).
7. Brownlie I. Principles of Public International Law. 6th ed. Oxford: Oxford University Press, 2003.
8. Criminal Code of Angola. URL: <http://www.wipo.int/wipolex/en/details.jsp?id=11018> (дата обращения: 25.02.2020).
9. Criminal Code of Bahamas. URL: <http://www.wipo.int/wipolex/en/details.jsp?id=15087> (дата обращения: 25.02.2020).
10. URL: <http://www.crime-research.ru/> (дата обращения: 25.02.2020).

¹ Положения Рамочного решения Совета 2002/475/JHA от 18 декабря 2008 года по европейскому ордеру на получение доказательств в виде предметов, документов и данных для использования в производстве по уголовным делам и инициативу Бельгии и других стран, касающуюся европейского ордера на расследование в уголовных делах, ОЖ С165/22 от 24 июня 2010 г.

11. URL: <http://www.planet360.info> (дата обращения: 25.02.2020).
12. URL: <http://www.rus.sectso.org/> (дата обращения: 25.02.2020).
13. URL: <http://www.un.org/ru/> (дата обращения: 25.02.2020).
14. UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5). URL: <http://www.uncjin.org/Documents/EighthCongress.html> (дата обращения: 25.02.2020).



Л.Я. Тарасова, канд. ист. наук

Барнаульский юридический институт МВД России

АНАЛИЗ СОСТОЯНИЯ НАСИЛИЯ В СЕМЬЕ В ПЕРИОД ПАНДЕМИИ COVID-19. СПОСОБЫ ЕГО ПРЕДУПРЕЖДЕНИЯ

«Семья – это общество в миниатюре, от целостности которого зависит безопасность всего большого человеческого общества»

Адлер Феликс, 1915 г.

На сегодняшний день проблема насилия в семье стала актуальной как никогда ранее. Одной из лакмусовых бумажек данного явления стала пандемия COVID-19.

В начале апреля 2020 г. генеральный секретарь ООН Антониу Гутерриш сообщил следующую информацию, что в условиях карантина и режима самоизоляции, введенных во многих странах для борьбы с распространением вируса COVID-19, в разы увеличилось количество случаев домашнего насилия. По некоторым подсчетам, осенью 2020 г. на карантине находилась треть населения всей планеты, или 2,6 млрд человек. О росте уровня домашнего насилия в условиях замкнутого пространства заявила в конце марта и генсек Совета Европы Мария Пейчинович-Бурич, сославшись на отчеты стран – членов СЕ. В марте-апреле 2020 г. об этом сообщали министр внутренних дел Франции Кристоф Кастанер, сотрудники британской общенациональной горячей линии для жертв домашнего насилия.

Однако следует заметить, что по официальным данным во время пандемии во Франции число обращений о домашнем насилии выросло на 30%, в Китае – более чем на 25%, в России обращения не носят массового характера.

По мнению правозащитников, это связано с тем, что жертвы боятся обращаться за помощью. Уполномоченный по правам человека Т. Москалькова пояснила, что в России сведения о домашнем насилии получают в основном от журналистов,

представителей некоммерческих организаций (различные кризисные центры). В период с 10 апреля 2020 г. количество жертв насилия и случаев насилия в семье увеличилось в 2,5 раза. Так, если в марте таких сообщений было 6054, то в апреле таких сообщений поступило более 13 тыс. [1]. По официальным данным МВД России, за 7 месяцев 2020 г. на 7% снизилось количество зарегистрированных преступлений против личности. Также сохранилась тенденция снижения уровня ряда других криминальных деяний, характеризующихся высокой степенью общественной опасности. В частности, число умышленных причинений тяжкого вреда здоровью уменьшилось на 4,6%, разбоев – на 19,2%, грабежей – на 12,9%. Зафиксировано снижение на 9,5% количества семейно-бытовых преступлений, в т.ч. на 13,6% меньше фактов умышленного причинения тяжкого вреда здоровью, на 11,8% – средней тяжести и на 7,4% – легкого вреда здоровью [2].

Согласно данным обзора МВД России от 1 сентября 2020 г., в ходе мониторинга ситуации, связанной с совершением правонарушений в семейно-бытовой сфере в условиях распространения новой коронавирусной инфекции, установлено, что, несмотря на введенные ограничительные меры (самоизоляцию), позитивная тенденция по данному виду преступности сохранилась. Число уголовно наказуемых деяний, совершенных в семейно-бытовой сфере, уменьшилось в мае на 6,3%, в июне – 12,6% [3].