К.А. Шафеев

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТВЕТСТВЕННОСТИ ЗА КИБЕРПРЕСТУПЛЕНИЯ В ПРАВЕ ЕВРОПЕЙСКОГО СОЮЗА

Аннотация. *В статье анализируется существующее правовое регулирование противодействия киберпреступности в праве Европейского союза, совершаемой онлайн с использованием преимуществ сети Интернет, а также выявляются тенденции и перспективы соответствующей стратегии кибербезопасности.*

Ключевые слова: *киберпреступления, сеть Интернет, право Европейского союза, уголовное право.*

Развитие информационных технологий влечет их внедрение во все сферы общественных правоотношений. Тем не менее упрощение повседневных операций, вызванное подобным научно-техническим прогрессом, неизменно приводит ко все более широкому использованию информационных технологий в преступных целях. В настоящее время практика показывает, что преступные действия могут совершаться как с использованием современной компьютерной техники и других электронных девайсов, так и посредством использования преимуществ сети Интернет. Соответственно, деятельность законодателей должна учитывать подобные тенденции.

Противодействие подобным преступлениям и привлечение лиц, совершивших подобные преступные деяния, к ответственности затруднены даже в рамках отдельных государств, поскольку зачастую преступников сложно идентифицировать из-за использования ими компьютерной техники и несовпадения места преступления с фактическим нахождением преступника в момент совершения. Тем более уголовное преследование преступлений такого рода будет затруднено в Европейском союзе, где киберпреступления чаще всего имеют трансграничный характер и могут воздействовать на интересы ЕС в целом.

Европейский союз обладает уникальной (в той мере, в какой это может относиться к международной организации) формой политико-правового устройства, которая в некоторых аспектах усложняет регу-

лирование различного рода правоотношений, а в некоторых аспектах их, наоборот, упрощает. Наиболее близкой аналогией здесь может выступать федеративное государство, где субъекты федерации сохраняют достаточно широкую компетенцию, а главные институции ЕС выступают в роли органов федеральной власти. При это достаточно легко усмотреть и соответствующий федеративный правовой конституционализм Европейского союза, при котором учредительные договоры и Хартия о фундаментальных правах исполняют роль конституционных актов, вторичное законодательство (регламенты, директивы, решения, рекомендации) выполняют функцию федеральных законов, а национально-правовые системы являются законодательными системами субъектов федерации, которые действуют до тех пор, пока не будут «вытеснены» вторичным законодательством вследствие гармонизационных процессов.

При этом нельзя сказать, что существуют все классические для национально-правовых систем отрасли права в «федеральном» восприятии права Европейского союза, поскольку ЕС является достаточно молодой международной организацией для того, чтобы полностью гармонизировать свою автономную правовую систему и привести все право государств-членов к единому «знаменателю».

Тем не менее в гармонизации и унификации уголовного права государств-членов и в создании единого уголовного права Европейского союза как наднациональной отрасли права европейские институции достигли заметных успехов. И все это, несмотря на довольно небольшой процент наднациональных нормативно-правовых актов, посвященных вопросам уголовного права, от общего числа законодательных актов ЕС.

1. Развитие уголовного права Европейского союза

Изначально гармонизация уголовного права Европейского союза началась на политическом уровне почти за 20 лет до того, как сам термин «Европейский союз» окончательно пришел на смену термину «Европейские сообщества». В 1975 г. на министерском уровне в рамках Европейского совета была организована группа TREVI[1], которая заложила основу европейского сотрудничества в сфере противодействия особо тяжким преступлениям, имеющим зачастую трансграничный

[1] (*англ.*) **T**errorism, **R**adicalism, **E**xtremism and **V**iolence **I**nternationally.

характер (терроризм, экстремизм и т.п.)[1]. При этом за время своей деятельности группа TREVI обозначила необходимость совершенно разных механизмов уголовного права, а также смежных областей. В частности, различные рабочие группы прорабатывали план гармонизации мер противодействия широкому кругу преступных действий, а также необходимых мер для подобной гармонизации: от футбольного хулиганства и безопасности ядерных установок до терроризма и полицейского и судебного сотрудничества по уголовным делам. После введения политики «трех опор» (см. далее) и взятия курса на усиленную политико-правовую интеграцию в начале 1990-х функционирование группы прекратилось ввиду распределения ее разнообразных задач между Европолом и другими *ad hoc* рабочими группами, деятельность которых касалась противодействия терроризму и другим опасным трансграничным преступлениям.

Следующим важным этапом на пути формирования единой отрасли уголовного права Европейского союза является принятие Маастрихтского договора в 1992 г., на основании которого ЕС получил три «опоры» – три главных направления и основания для продолжения европейской политико-правовой интеграции[2].

Первой опорой являлись Европейские сообщества, в рамках которых проводилась интеграция по направлениям создания единого экономического рынка, европейских конкурентных правил, единой политики охраны окружающей среды, а также валютного союза.

Второй опорой стала Общая внешняя политика и политика безопасности, которая обозначала роль Европейского союза в миротворчестве, правах человека, соответствующей помощи третьим государствам и т.п., т.е. очерчивала роль ЕС на мировой арене, несмотря на пока отсутствующую правосубъектность.

Третья опора изначально была обозначена как «Правосудие и внутренние дела» (англ. *Justice and Home Affairs*). Позже, после вступления в силу Амстердамского договора, в 1999 г. она была переименована в «Полицейское и судебной сотрудничество по уголовным делам» (англ. *Police and Judicial Co-operationin Criminal Matters*), что точнее отражает направление гармонизации в данной области. Соответственно в рамках данной опоры государства-члены обеспечивали сотрудниче-

[1] *Tony Bunyan*. Trevi, Europol and the European state (http://www.statewatch.org/news/handbook-trevi.pdf, свободный (загл. с экрана)).

[2] Treaty of Maastricht on European Union // Document information (http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:xy0026, свободный (загл. с экрана)).

ство судебных органов по вопросам уголовных дел, а также сотрудничество полицейских органов для противодействия трансграничным преступлениям (терроризм, торговля наркотиками, организованная преступность и т.п.).

Также в этот период принимались пятилетние программы действия для развития кооперации государств-членов в области правосудия и внутренних дел: Тамперская программа (1999 г.)[1] обозначила направления по созданию единой миграционной политики ЕС, европейского пространства правосудия, борьбы с трансграничной преступностью и внешней политики в данной области; Гаагская (2005 г.) и Стокгольмская (2010 г.) программы конкретизировали интеграцию государств-членов в вышеназванных направлениях.

После вступления в силу Лиссабонского договора в декабре 2009 г. система опор была упразднена, однако Европейский союз в силу своей появившейся правосубъектности получил некоторые компетенции в сфере уголовного права.

Статья 67 Договора о функционировании Европейского союза[2] (далее – ДФЕС) устанавливает пространство свободы, безопасности и правосудия, учитывая фундаментальные права человека и различия в правовых системах и традициях государств – членов. При этом безопасность и правосудие должны обеспечиваться посредством мер по предупреждению преступности и взаимного признания и исполнения судебных решений по уголовным делам, путем кооперации полицейских органов и иных компетентных органов, а также при необходимости гармонизацией уголовных законов государств-членов.

На основании ст. 4 ДФЕС в рамках пространства свободы, безопасности и правосудия ЕС имеет совместную с государствами-членами компетенцию, это означает, что и ЕС как наднациональная структура, и государства-члены могут принимать нормативно-правовые акты в данной области. Но (если проводить параллель с европейским федерализмом) в области совместной компетенции действует правило «вытеснения», которое означает, что, если какие-либо правоотношения были гармонизированы институциями ЕС на общесоюзном уровне, государства-члены теряют свое право нормотворческой деятельности

[1] Tampere. Kick-start to the EU's policy for justice and home affairs (http://ec.europa.eu/councils/bx20040617/tampere_09_2002_en.pdf, свободный (загл. с экрана)).

[2] Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012. P. 47–390.

в данной области. Это значимо для сферы уголовного права, поскольку благодаря этому ЕС обладает компетенцией определить необходимый минимум уголовного законодательства государств-членов. Такая практика устоялась в отношении конкретного перечня преступных деяний, напрямую указанных в учредительных договорах.

2. Европреступления

Статья 83 ДФЕС подтверждает компетенцию ЕС по установлению минимума состава и санкций в отношении определенных особо тяжких преступлений, часто носящих трансграничный характер, – так называемых европреступлений.

К подобного рода преступным деяниям относятся терроризм, торговля людьми, сексуальная эксплуатация женщин и детей, торговля оружием, торговля наркотиками, отмывание денег, коррупция, подделка платежных средств, компьютерные преступления и организованная преступность. Данный список носит исчерпывающий характер, однако может быть расширен Советом ЕС, действующим единогласно после получения согласия Европейского парламента. При этом на данный момент минимум состава и санкций гармонизирован для всех перечисленных преступлений (за исключением торговли оружием), это означает, что государства-члены не могут сделать свое уголовное законодательство мягче установленных стандартов в рамках противодействия подобным преступлениям и применения мер ответственности к лицам, их совершившим.

Также стоит отметить, что к подобного рода преступным деяниям на основании указанных критериев (особая опасность, трансграничный характер) можно отнести преступления против финансовых интересов Европейского союза (к примеру, подделка евро, ст. 325 ДФЕС); преступлений, затрудняющих единообразное применение политики ЕС в государствах-членах (ст. 83(2) ДФЕС). В этих областях ЕС также имеет компетенцию устанавливать обязательное уголовное преследование подобных преступлений в государствах-членах и минимум состава и санкций.

Подобные компетенции, закрепленные в учредительных договорах, воплощаются путем принятия секторального вторичного законодательства (в основном Директив и Рамочных решений), которое государства – члены обязаны имплементировать в свои национально-правовые системы в течение определенного времени.

3. *Status-quo* противодействия киберпреступлениям

Развитие информационных технологий сделало все аспекты человеческих жизней практически зависимыми от различных электронных девайсов и наличия доступа в сеть Интернет. В настоящий момент сложно представить, к примеру, ведение бизнеса без сайта в сети Интернет, без общения онлайн с контрагентом по договору или без электронного перевода платежей.

Киберпреступность имеет гораздо более значительные масштабы: на сегодняшний день объектом подобных преступных кибердеяний могут стать не только экономические интересы человека, но и, например, его личная информация. Европейский союз, где ввиду отсутствия внутренних границ преследование подобных преступлений осложнено их постоянным трансграничным характером, осознал соответствующие вызовы, стоящие перед ним с законодательной точки зрения, и ответил на угрозу роста киберпреступности своевременной стратегией по кибезащите интересов Союза и его граждан.

Киберпреступления вне зависимости от объекта преступных деяний объединяют два признака: во-первых, все они совершаются онлайн, т.е. с использованием доступа в сеть Интернет; во-вторых, все они совершаются с использованием электронных коммуникационных сетей и информационных систем.

По объектному составу все совершаемые киберпреступления можно разделить на три большие группы: 1) преступления, связанные с информационными возможностями сети Интернет (хакерские атаки на информационные сети, фишинг (кража паролей) и т.п.); 2) онлайн-мошенничество; 3) онлайн-хранение неправомерной информации (детская порнография, информация, подстрекающая к расовой ненависти, терроризму и ксенофобии и т.п.).

3.1. Преступления, связанные с информационными возможностями сети Интернет

Что касается первой группы преступлений, связанной прежде всего с использованием информационных преимуществ сети Интернет, то в данных случаях преступники осуществляют кражу информации, которая обычно находится в закрытом доступе, путем хакерских атак на информационные сети или фишинга, т.е. кражи паролей при помощи фальшивых фишинговых сайтов или программ, где потерпевшие,

заблуждаясь, вводят свою личную информацию (обычно пароли или реквизиты банковских карт).

Противодействие подобным киберпреступлениям было урегулировано одним из первых на общеевропейском уровне.

Еще в 2002 г. была принята первая редакция Директивы 58/ЕС, касающаяся обработки персональных данных и защиты неприкосновенности частной жизни в сфере электронных коммуникаций[1] (Директива о неприкосновенности частной жизни и электронных коммуникациях). Эта Директива в первую очередь ориентирована на защиту прав пользователей, под которыми понимаются любые физические лица, которые используют общедоступные средства электронной коммуникации в личных или коммерческих целях.

Защита пользователей осуществляется путем установления позитивного обязательства поставщиков общедоступных средств электронной коммуникации (провайдеров) по принятию надлежащих технических и организационных мер для обеспечения безопасности предоставляемых ими услуг. Подобные меры должны отвечать соответствующему уровню риска стать жертвой релевантных киберпреступлений и должны как минимум включать обеспечение доступа к личной информации только путем авторизации; защиту личных данных от случайного или неправомерного удаления, изменения, обработки, доступа или раскрытия; и обеспечение реализации соответствующей политики безопасности в отношении обработки персональных данных. Также провайдеры обязаны своевременно сообщать пользователям о любом повышении рисков и случаях взломов и кражи их личной информации.

Государства-члены, в свою очередь, обязаны не допускать случайного или неправомерного нарушения конфиденциальности электронных коммуникаций. Любая запись или хранение электронных коммуникаций возможны лишь при даче ясного согласия на это субъектами коммуникации или на основании закона. Вместе с тем у государств-членов также появляется обязанность по обеспечению соответствия национальных систем электронной коммуникации стандартам Европейского союза.

Еще одним важным нормативно-правовым актом ЕС в сфере противодействия преступлениям, связанным с информационными воз-

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002. P. 37–47.

можностями сети Интернет, стала Директива 2013/40/EU об атаках на информационные системы[1]. Директива устанавливает минимальные определения и санкции для преступлений, связанных с атаками на информационные системы в государствах-членах, а также создает условия для сотрудничества судебных и полицейских органов в преследовании подобных преступных деяний.

На основании данной Директивы государства-члены должны криминализировать следующие уголовные составы: незаконный доступ к информационным системам, незаконное вмешательство в функционирование информационных систем, незаконная обработка данных (например, удаление, копирование, изменение и т.п.) и незаконный перехват передачи данных. Также государства-члены обязаны обеспечить уголовное преследование лиц, производящих, продающих, покупающих, импортирующих и распространяющих орудия для подобных преступлений: компьютерные программы, пароли, коды доступа к информационным системам и любая соответствующая информация. Уголовно преследоваться должны соучастники, а также лица, которые покушались на совершение незаконного вмешательства в функционирование информационных систем и незаконную обработку данных.

Наказания должны назначаться, учитывая принципы эффективности, пропорциональности и превентивности. При этом санкции назначаются по правилу «максимума-минимума», при котором Европейский союз устанавливает необходимый минимум максимальных санкций. Соответственно, все вышеперечисленные составы, будучи криминализированными в государствах-членах, должны предусматривать максимальные санкции в виде лишения свободы на срок не менее двух лет. Если незаконное вмешательство в функционирование информационных систем или незаконная обработка данных были совершены умышленно и с нарушением функционирования большого количества информационных систем или больших объемов данных, то максимальные санкции должны предусматривать лишение свободы на срок не менее трех лет. Эти же преступные составы наказываются максимальными санкциями в виде лишения свободы на срок не менее пяти лет при наличии следующих квалифицирующих признаков: если они были совершены преступной организацией; если они повлекли серьезный ущерб; если преступление было совершено в отношении

[1] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJ L 218, 14.08.2013. P. 8–14.

важной инфраструктурной информационной системы. Кроме того, государства – члены должны установить свою юрисдикцию в отношении подобных преступлений, если преступление или его часть были совершены на территории государства-члена; если преступление было совершено гражданином государства-члена; если преступник находится на территории государства-члена; и если информационная система, против которой было совершено преступление, находится на территории государства-члена. Также после соответствующего уведомления Европейской комиссии государство-член имеет право расширить свою юрисдикцию и на те случаи, когда преступник имеет свое обычное местожительство на территории государства-члена и когда преступление было совершено в пользу юридического лица, которое зарегистрировано в данном государстве-члене.

3.2. Онлайн-мошенничество

Основным нормативно-правовым актом Европейского союза в рамках противодействия онлайн-мошенничеству и смежных с ним преступных деяний является Рамочное решение Совета ЕС 2001/413/ JHA о противодействии мошенничеству и подделке безналичных платежных средств[1].

Это решение обязывает государства-члены криминализировать практически все основные уголовные составы, так или иначе связанные с безналичными расчетами: кража банковских карт, фальсификация платежных инструментов, умышленное использование заведомо краденых платежных средств и т.п. Государства обязаны криминализировать ряд преступлений, относящихся к сфере киберпреступлений, совершаемых онлайн посредством сети Интернет: получение выгоды за счет трансфера денежных средств другого лица без соответствующих прав на обработку (введение, изменение, удаление, копирование) персональных данных и соответствующих прав на вмешательство в функционирование компьютерной системы или программы. Также уголовно преследоваться должны изготовление, продажа, покупка и передача компьютерных программ, предназначенных для совершения вышеназванных киберпреступлений. Соответственно должны преследоваться соучастие и покушения на эти преступления.

[1] 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. OJ L 149, 02.06.2001. P. 1–4.

Что касается гармонизации санкций в отношении данной категории киберпреступлений, то нельзя с уверенностью сказать, что эта область достаточно гармонизирована. Это связано с тем, что, помимо необходимости соответствия наказания принципам эффективности, пропорциональности и превентивности, в Рамочном решении указано лишь на возможность применения санкций в виде лишения свободы (с допустимостью экстрадиции) «в серьезных случаях», без указания какого-либо минимума такого лишения. Вследствие этого определение санкций практически полностью передано на усмотрение государств-членов.

При этом государства-члены обязаны установить свою обязательную юрисдикцию в отношении уголовного преследования киберпреступлений подобного рода, если: преступление или его часть были совершены на территории государства-члена; преступление было совершено гражданином государства-члена; преступление было совершено в пользу юридического лица, чей административный центр находится на территории данного государства-члена.

3.3. Онлайн-хранение неправомерной информации

Сеть Интернет помимо общеизвестной полезности является самым большим хранилищем информации. Но не всегда хранимая информация является правомерной. И, к сожалению, широко распространены ситуации, при которых хранение неправомерной информации нарушает права особо уязвимой категории граждан – детей.

Именно поэтому в рамках вторичного законодательства Европейским союзом была разработана и принята Директива 2011/92/EU о противодействии сексуальному надругательству и сексуальной эксплуатации детей и детской порнографии[1].

Помимо необходимости криминализировать ряд основных преступлений, связанных с детской порнографией и детской сексуальной эксплуатацией, у государств-членов появляется обязательство по криминализации нескольких киберпреступлений в данной сфере, которые появились совсем недавно ввиду развития информационных технологий и сети Интернет. Так, криминализации подлежат

[1] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. OJ L 335, 17.12.2011. P. 1–14.

любые попытки встретиться с ребенком, совершенные при помощи средств информационных и коммуникационных технологий, с намерением совершить любое преступление из группы преступлений, связанных с сексуальной эксплуатацией детей. Подобные преступления должны наказываться в государствах-членах лишением свободы на максимальный срок не менее одного года. Также уголовно преследоваться должно и покушение на подобное преступление, совершенное при помощи средств информационных и коммуникационных технологий. Все электронные девайсы, с помощью которых были совершены подобные преступные деяния, подлежат конфискации.

Также государства-члены обязаны принять все необходимые меры для оперативного удаления веб-страниц, содержащих или распространяющих детскую порнографию, если серверы данного веб-сайта находятся на их территории; и все попытки, необходимые для удаления данных веб-сайтов, если их серверы находятся за пределами территории государств-членов. Также могут устанавливаться соответствующие внутренние меры по блокировке сайтов, содержащих или распространяющих детскую порнографию, при условии соблюдения принципов эффективности, пропорциональности и прозрачности.

Что касается установления юрисдикции, то государства-члены обязаны установить юрисдикцию в отношении всех киберпреступлений, сопряженных с онлайн-хранением неправомерной информации, если все преступление или его часть были совершены на его территории и если преступление было совершено гражданином данного государства-члена.

Также с условием уведомления Европейской комиссии государства-члены могут расширить свою юрисдикцию на ситуации, когда киберпреступления были совершены против гражданина данного государства-члена или лица, имеющего свое постоянное местожительство на территории данного государства-члена; когда киберпреступление было совершено в пользу юридического лица, зарегистрированного в установленном законом порядке на территории данного государства-члена; когда субъект киберпреступления имеет свое обычное местожительство на территории данного государства-члена. При этом киберпреступление считается совершенным на территории государства-члена, даже если на его территории всего лишь находятся информационные и коммуникационные технологии, при помощи которых киберпреступление было совершено.