АНАЛИЗ СОВРЕМЕННОГО ПРАВА

IP & Digital Law

ПРАВО В СФЕРЕ ИНТЕРНЕТА

СТАТУТ

Анализ современного права

Сборник статей

Право в сфере Интернета

«Статут»
2017

УДК 004.738.5
ББК 67.401.114

Сборник статей

Право в сфере Интернета / Сборник статей — «Статут», 2017 — (Анализ современного права)

ISBN 978-5-8354-1417-8

Четырнадцатый сборник из серии «Анализ современного права» объединяет статьи, посвященные правовому регулированию отношений в Интернете. В него вошли работы, касающиеся вопросов ответственности за киберпреступления, соблюдения антимонопольного законодательства, регулирования отношений по поводу персональных данных, в том числе с участием информационных брокеров, нарушений в социальных сетях, особенностей рекламы и торговли в сети Интернет, признания информации, запрещенной к распространению, перспектив использования технологии блокчейн, регистрации и использования доменных имен и др. Также в сборнике рассматривается проблематика изменения частного права под влиянием развития сети Интернет и, в частности, анализируются договоры присоединения к многопользовательской игре, особенности электронной формы различных договоров, защита авторских прав в цифровой среде (гиперссылки, мемы, лицензии Creative Commons, ключевые слова), аспекты частноправовых процедур рассмотрения споров. Для судей, адвокатов, практикующих юристов, научных работников, преподавателей, аспирантов и студентов юридических факультетов, а также всех тех, кого интересуют проблемы развития российского права и вопросы применения действующего законодательства. Сборники серии «Анализ современного права» – это издания, в которых публикуются работы на актуальные темы как представителей университетской среды, так и юристов-практиков. В сборник могут быть включены работы различных авторов, в том числе не имеющих ученых степеней.

УДК 004.738.5

ББК 67.401.114

ISBN 978-5-8354-1417-8

Содержание

Право в сфере Интернета: Сборник статей Руководитель авторского коллектива и ответственный редактор доктор юридических наук М.А. Рожкова

Предисловие

На протяжении длительного времени юристы спорят о том, нужно ли для отношений, возникающих в Интернете, новое, самостоятельное правовое регулирование либо вполне допустимо несколько скорректировать существующее законодательство с тем, чтобы его можно было применить к Интернету. Причем приверженцы идеи разработки специального законодательства для регламентации интернет-отношений не останавливаются на предложениях о новых специальных законах в обозначенной сфере, а говорят о необходимости выделения в отдельную отрасль норм, регулирующих правоотношения в Интернете.

Не вдаваясь в эту дискуссию, хотелось бы поддержать правоведов, не усматривающих проблемы в распространении действующего законодательства на интернет-отношения (хотя, бесспорно, это потребует внесения соответствующих корректив в существующие НПА). Объяснение этому весьма простое и оно всецело подтверждается содержанием настоящего сборника: Интернет проникает во все сферы нашей жизни, «позволяя» возникать отношениям, которые подпадают под регулирование норм различных отраслей законодательства – административного, уголовного, гражданского, конкурентного и т.д.

В таких условиях принятие самостоятельных законов, регламентирующих только отношения, возникающие в Интернете, будет дублировать нормы уголовного, административного, гражданского и иного законодательства, что повлечет за собой известные сопутствующие проблемы. Это и несогласованность законодательных текстов, и вопросы разграничения сфер регулирования, и необоснованные различия в регулировании схожих случаев, а также иные коллизии. Поэтому более верным и, что немаловажно, более простым решением будет дополнение существующих законов нормами, потребность в которых демонстрирует практика.

Настоящий сборник, конечно, не претендует на постановку и освещение всех проблем, возникающих в интернет-среде. Его основная задача состоит скорее в том, чтобы обозначить актуальные направления в рассматриваемой сфере.

Эта задача сборника неожиданно совпала с одной из целей Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности (*IP&ITLAW)* – выявление перспективных направлений в области правовой охраны и защиты прав в цифровой среде, в частности, прав на персональные данные, доменные имена, интеллектуальную собственность, виртуальную собственность и др. Это и объясняет то, что в настоящем сборнике публикуются в том числе работы победителей и некоторых участников 2 Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности (*IP&ITLAW— 2017).*

В развитие сказанного надо отметить, что темы конкурсных работ 3 Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности *(IP&ITLAW— 2018)* также пересекаются с тематикой готовящегося пятнадцатого сборника серии «Анализ современного права» (его рабочее название – «E-commerce, торговля онлайн и оффлайн (правовые аспекты)»; см. *www.asp.wzhkova.com).* Поэтому предполагается,

что наиболее интересные конкурсные работы также будут опубликованы в следующем сборнике данной серии.

В связи со сказанным приглашаем молодых исследователей (аспирантов, студентов) принять участие в конкурсе *LP&LTLAW – 2018* (см. *www.2018.ipclub.in*). Этот конкурс проводится *IP CLUB* совместно с Координационным центром национального домена сети Интернет при поддержке Комитета Государственной Думы по информационной политике, информационным технологиям и связи.

В завершение хотелось бы напомнить потенциальным авторам, что срок принятия статей в следующий сборник настоящей серии, который, как указывалось, носит рабочее название «E-commerce, торговля онлайн и оффлайн (правовые аспекты)», – до 1 апреля 2018 г. Ознакомиться с условиями публикации можно на странице www.asp.*wzhkova.com*

М.А. Рожкова, д.ю.н.,

эксперт Российской Академии Наук, член Экспертного Совета Комитета Государственной Думы по информационной политике, информационным технологиям и связи, президент IP CLUB

Указатель сокращений

АПК РФ Арбитражный процессуальный кодекс Российской Федерации

АС Арбитражный суд

ААС апелляционный арбитражный суд

ВАС РФ Высший Арбитражный Суд Российской Федерации (в настоящее время упразднен)

ВС РФ Верховный Суд Российской Федерации

ГГУ Германское гражданское уложение

ГК Гражданский кодекс

ГК РФ Гражданский кодекс Российской Федерации

ГПК РФ Гражданский процессуальный кодекс Российской Федерации

Закон о персональных данных Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Закон об информации Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

ЕСПЧ Европейский суд по правам человека

КАС РФ Кодекс административного судопроизводства Российской Федерации

КоАП РФ Кодекс Российской Федерации об административных правонарушениях

КС РФ Конституционный Суд Российской Федерации

Конвенция по правам человека Конвенция о защите прав человека и основных свобод

Концепция развития гражданского законодательства Концепция развития гражданского законодательства Российской Федерации (Вестник ВАС РФ. 2009. № 11. С. 6–99)

ОО общество с ограниченной ответственностью

ТК РФ Трудовой кодекс Российской Федерации

УК РФ Уголовный кодекс Российской Федерации

ФАС Федеральный арбитражный суд

ФГК Французский гражданский кодекс

ФЗ Федеральный закон

Правовое регулирование ответственности за киберпреступления в праве Европейского союза (Вильнюс, Литва)

Кирилл Азизавич Шафеев

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 политике-правового устройства, которая в некоторых аспектах усложняет регулирование 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 характер (терроризм, экстремизм и т.п.)[2]. 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 [3].

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 сотрудничество 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.)[4] обозначила направления по созданию единой миграционной политики ЕС, европейского пространства правосудия, борьбы с трансграничной преступностью и внешней политики

---

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

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

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

[4] 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)).

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[5](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 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.

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

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 киберзащите 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[6] (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 жерт-

[6] 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.

вой 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 возможностями сети Интернет, стала Директива 2013/40/EU об атаках на информационные системы[7]. 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 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

[7] 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.

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[8].

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.

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 [9].

---

[8] 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.

[9] 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,

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 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.

3.4. Иные инициативы ЕС в области противодействия киберпреступлениям

В мае 2015 г. Европейская комиссия под председательством Жан-Клода Юнкера инициировала создание европейского Цифрового единого рынка (англ. *Digital Single Market)* – сегмента европейского Единого рынка, в рамках которого свободное передвижение товаров, услуг, лиц и капитала могло бы осуществляться с постоянным доступом онлайн в условиях честной конкуренции и защиты личных данных вне зависимости от гражданства или местонахождения[10]. Однако необходимые основы для формирования безопасного цифрового рынка были заложены еще в 2013 г., когда Европейский парламент, Совет Европейского союза, Европейский

17.12.2011. P. 1 – 14.

[10] Digital Single Market // official site of European Commission (https://ec.europa.eu/dig-ital-single-market/en/digital-single-market (загл. с экрана)).

экономический и социальный комитет и Комитет регионов совместно предложили Стратегию кибербезопасности ЕС[11].

Помимо необходимых основ по защите личных данных для формирования Цифрового единого рынка, поводом для формирования Стратегии кибербезопасности ЕС стала серьезная обеспокоенность институций ЕС соблюдением фундаментальных прав человека, в том числе и онлайн. Киберпреступления – весьма специфический и труднорегулируемый вид преступных деяний, где объектом преступления помимо экономических интересов граждан является их право на защиту частной и семейной жизни. Киберпространство должно соответствовать таким стандартам, при которых права граждан онлайн не только бы защищались, но и могли бы свободно реализовываться самими гражданами. Свобода слова является одной из главнейших демократических ценностей, а поскольку сеть Интернет является ключевым информационным источником на сегодняшний день, невозможно представить современное демократическое общество без возможности свободного при условии правомерности выражения мнения онлайн.

Кибербезопаность Европейского союза предполагает реализацию на основе ряда принципов, каждый из которых учитывает как позитивные, так и негативные аспекты современного роста информационных технологий.

Первостепенным является защита фундаментальных прав человека: свободы слова, неприкосновенности личной жизни и персональных данных. При этом реализация и защита прав человека онлайн должна происходить с учетом стандартов Хартии о фундаментальных правах ЕС[1] – основополагающего нормативно-правового акта по правам человека в Европейском союзе, имеющего юридическую силу учредительных договоров.

Не менее важным является соблюдение принципа равенства, а именно установление свободного доступа в сеть Интернет для всех граждан Союза и осуществления в отношении всех граждан единых стандартов кибербезопаности.

Также стратегия кибербезопасности должна реализовываться с соблюдением принципа «антимонопольности» управления, что подразумевает возможность оказания услуг по предоставлению доступа в сеть Интернет не только государственными организациями, но и частными компаниями. Подобный публично-частный дуализм управления должен реализовываться на основании принципа разделения ответственности, на основании которого как публичные, так и частные провайдеры должны нести ответственность перед законом и соответствовать общепринятым стандартам кибербезопасности.

Стратегия ЕС в области кибербезопасности осуществляется по пяти основным направлениям, отражающим как внутрисоюзные потребности киберпространства, так и международные тенденции в этой области.

Первое направление включает достижение устойчивого уровня защиты от киберугроз. Под этим понимается установление минимальных стандартов Сетевой и информационной безопасности, которые были бы обязательными как для частных, так и для публичных акторов, координация и сотрудничество национальных компетентных органов, отвечающих за кибербезопасность, увеличение технического уровня частного сектора в данной области, а также развитие общеевропейских инициатив в сфере кибербезопасности.

Вторым направлением является непосредственное снижение количества совершаемых киберпреступлений путем принятия эффективного и строгого законодательства в сфере противодействия киберпреступлениям, расширения числа оперативных мероприятий и сотрудничества полицейских и судебных органов государств-членов.

[11] Cyber Security Strategy of the European Union: An open, safe and secure cyberspace. Joint communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions /* JOIN/2013/01 final */

Третье направление вводит кибербезопасность в рамки Общей внешней политики и политики безопасности. В рамках данного направления планируется открытие диалога между частным и военным секторами в области кибербезопасности, более стандартизированное обучение соответствующего персонала, сотрудничество с международными партнерами (к примеру, НАТО).

Четвертое направление включает в себя развитие индустриальных и технологических ресурсов для обеспечения средств кибербезопасности.

И, наконец, пятое направление заключается в создании согласованной международной политики в области кибербезопасности, которая бы продвигала основные ценности Европейского союза в данной области (фундаментальные права человека, свобода Интернета, защита частной и семейной жизни и т.п.). В рамках данного направления ожидается сотрудничество с НАТО, ОБСЕ, ООН, АСЕАН и другими ключевыми международными межправительственными организациями.

Также в рамках поддержки положений Стратегии кибербезопасности ЕС в январе 2013 г. Европол создал Европейский центр по борьбе с киберпреступностью[12] (далее – ЕСЗ).

ЕСЗ является специальным отделом Европола, в компетенцию и задачи которого входит усиление правоохранительных органов в ответ на угрозу киберпреступности в Европейском союзе и, таким образом, защита прав граждан, предприятий и государств – членов от онлайн-преступности. Для этого ЕСЗ разрабатывает методики экспертиз в случаях совершения киберпреступлений, собирает и классифицирует информацию о новых способах совершения киберпреступлений, разрабатывает стратегии для осуществления сотрудничества национальных полицейских органов, а также рекомендует порядок проведения и виды оперативных мероприятий в случае совершения киберпреступлений.

ЕСЗ тесно сотрудничает с Агентством ЕС по сетевой и информационной безопасности, которое учреждено после вступления в юридическую силу Регламента No 460/2004[13]. Главной целью данного Агентства является разработка и помощь институциями государствам-членам и представителям экономического сектора в имплементации стандартов сетевой и информационной безопасности для надлежащего функционирования внутреннего рынка ЕС.

Отдельно стоит упомянуть нормативно-правовые акты, которые станут частью системы права Европейского союза и вступят в свою законную силу в скором будущем.

В 2016 г. был принят новый Регламент 2016/679 об общей защите данных[14]. Регламент представляет собой масштабный и объемный нормативно-правовой акт, призванный установить стандарты обработки данных в Европейском союзе, при которых гарантировались бы все фундаментальные права граждан ЕС, а также принцип законности. В документе содержатся такие новеллы права прав человека и кибербезопаности, как право «быть забытым», право на изменение информации, право на переносимость данных и т.п. Но, несмотря на то что регламенты обладают прямым действием и не нуждаются в имплементации в национально-правовые системы, в законную силу Регламент 2016/679 вступит только 25.05.2018.

---

[12] About // EuropeanCybercrimeCentre (https://www.europol.europa.eu/about-europol/ european-cybercrime-centre-ec3 (загл. с экрана)).

[13] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). Official Journal L 077, 13.03.2004. P. 0001—0011.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 04.05.2016. P. 1—88.

4. Ответственность юридических лиц

На данный момент существует очевидная тенденция по включению в национальные уголовные кодексы института уголовной ответственности юридических лиц. Страны Европейского союза не стали исключением: институт уголовной ответственности юридических лиц существует, к примеру, в Литве (ст. 20 Уголовного кодекса Литовской Республики[15]), Франция (ст. 121-2 Уголовного кодекса Французской Республики[16]) и т.д.

Однако на данный момент не представляется возможным гармонизировать институт уголовной ответственности юридических лиц на общесоюзном уровне ввиду слишком больших различий в правовом регулировании данного вопроса в государствах-членах. Соответственно в наднациональном праве Европейского союза нет института уголовной ответственности юридических лиц, но предусматривается ответственность юридических лиц за преступления. При этом государства-члены обязаны преследовать юридические лица за совершение киберпреступлений, однако вид преследования (административное или уголовное), а также виды санкций остаются на усмотрение государств-членов.

При этом, указывая на возможность ответственности юридических лиц за преступления, европейские институты всегда оставляют рекомендательную норму, содержащую возможные административные и уголовные виды санкций, применимые к юридическим лицам. Норма ответственности юридических лиц за преступления содержится в неизменном виде практически в каждом нормативно-правовом акте, который относится к уголовному праву ЕС, и преследование киберпреступлений, совершаемых в и при помощи сети Интернет, не является исключением.

Ответственность юридических лиц за преступления наступает при наличии определенных критериев и при этом не исключает возможности уголовного преследования физического лица, непосредственно совершившего преступные деяния. Основания ответственности юридических лиц за киберпреступления можно условно разделить на обязательные и дискреционные. При наличии всех обязательных оснований государства-члены обязаны привлечь юридическое лицо к ответственности; если установлены все дискреционные основания, то государство-член должно решить вопрос о необходимости привлечения юридического лица к ответственности.

Под обязательными основаниями понимаются: совершение преступления физическим лицом; совершение преступления в пользу и в интересах юридического лица, наличие у физического лица руководящей позиции. Руководящая роль выражается в наличии полномочий по представлению юридического лица, по совершению юридических действий от имени юридического лица, а также наличии контролирующих полномочий в целом. При этом не имеет значения, в каком качестве выступает физическое лицо в момент совершения преступления.

Дискреционные основания включают в себя: совершение преступления физическим лицом (а именно любым, кто представляет интересы юридического лица), совершение преступления в пользу юридического лица, отсутствие достаточного контроля со стороны руководящего лица.

Стандартным положением для данного института уголовного права является государственный иммунитет и иммунитет международных публичных организаций: меры ответственности юридических лиц не могут быть применены к государству, государственным предпри-

---

[15] Lietuvos Respublikosbaudziamojokodekso (https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/TAIS.111555, свободный (загл. с экрана)).

[16] Codepenal (https://www.legifrance.gouv.fr/affichCode.do;jsessionid=F06BB691FF16DDFE9DF58E6822AEA8B9.tpdilallv_1?idSectionTA=LEGISCTA000006149817&cidTexte=LEGITEXT000006070719&dateTexte=20170331, свободный (загл. с экрана)).

ятиям, институциям государства и местной власти, а также к международным публичным организациям.

Также предусматриваются следующие рекомендательные санкции: штраф, временное лишение права деятельности, ликвидация, запрет на предоставление государственной помощи, временный запрет на участие в государственных закупках (в том числе там, где покупателем выступает ЕС или его институция).

Заключение

Таким образом, правовое регулирование противодействия киберпреступности в Европейском союзе является достаточно широким и в первую очередь направленным на защиту потерпевших, их прав на неприкосновенность частной и семейной жизни, а также на защиту личной информации. Стоит отметить, что европейское законодательство в данной области учитывает все опасные тенденции развития информационных и коммуникационных технологий, а также совершение уже ранее известных уголовному законодательству государств-членов преступных деяний, получивших принципиально новую форму ввиду использования для их совершения информационных удобств сети Интернет.

Несмотря на тот факт, что киберпреступность – явление весьма молодое, европейские институции значительно преуспели в вопросе правового регулирования противодействия, которое не ограничивается нормативно-правовыми актами уголовного права. В частности, благодаря процессам гармонизации на данный момент уже можно говорить о сложившихся стандартах обработки информации в ЕС, а также о достаточном соблюдении прав человека в этой области, что на практике дополняет действие Хартии о фундаментальных правах, которая устанавливает общие положения о неприкосновенности частной, семейной жизни и личной информации.

Что касается уголовного права Европейского союза в сфере противодействия киберпреступлениям в сети Интернет, то на сегодняшний день можно наблюдать достаточно эффективную гармонизацию законодательства государств-членов посредством имплементации вторичного законодательства ЕС. Это законодательство устанавливает минимум определений и санкций (преимущественно в виде лишения свободы и конфискации электронных девайсов, с помощью которых были совершены релевантные киберпреступления) для наиболее распространенных категорий преступных деяний, сопряженных с информационными возможностями сети Интернет, онлайн-мошенничеством и онлайн-хранением неправомерной информации.

Стоит отметить, что применительно к онлайн-хранению неправомерной информации на общеевропейском уровне эффективно урегулировано лишь противодействие хранению информации, касающейся сексуальной эксплуатации детей. Это, безусловно, является значительным для системы уголовного права ЕС, поскольку в данном случае защищаются права наиболее уязвимых граждан.

Вместе с тем в перспективе необходимо развивать регулирование противодействия онлайн-хранения информации экстремистского характера. На данный момент противодействие разжиганию ненависти по любым мотивам регулируется Рамочным решением Совета 2008/913/JHA[17], однако данный нормативно-правовой акт включает в преступные составы лишь те преступные деяния, которые были совершены публично, оставляя за сферой своего действия преступления такого рода, совершенные при помощи средств онлайн-коммуникации и сети Интернет.

Противодействие онлайн-мошенничеству также весьма эффективно. Несмотря на то что правовое регулирование на общеевропейском уровне основывается лишь на одном нормативно-правовом акте, все самые последние тенденции киберпреступности в данной сфере отслеживаются ЕСЗ, который осуществляет сотрудничество с полицейскими органами всех государств-членов, что позволяет оперативно осуществлять мероприятия для предотвращения онлайн-мошенничества.

[17] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. OJ L 328, 06.12.2008. P. 55-58.

Самым проблемным полем остается группа киберпреступлений, связанных с информационными возможностями сети Интернет, поскольку передвижение информации онлайн связано, во-первых, с огромными объемами, а во-вторых, с каждодневным появлением новых возможностей для преступников возобновить и изменить свою преступную деятельность, выходящую за пределы существующего уголовного законодательства. В отличие от основных видов преступлений, таких как фишинг или хакерские атаки (которые урегулированы достаточно новыми Директивами), вопрос свободного движения информации в ЕС в целом остается открытым – эта сфера на данный момент не урегулирована, но, возможно, ситуация улучшится с вступлением в силу Регламента об общей защите данных.

Таким образом, правовое регулирование противодействия киберпреступлениям в Европейском союзе характеризуется разносторонним и многоуровневым подходом, сочетающим как нормативно-правовые акты «мягкого» права, так и регламенты, директивы и рамочные решения, обязательные для государств-членов. В целом уже на данном этапе развития этого сегмента уголовного права ЕС существующая практика и модель правового регулирования, а также существующие стандарты в этой области могут быть переняты государствами, не входящими в ЕС, в качестве образца для реформирования собственных систем уголовной юстиции в сфере противодействия киберпреступлениям.

Пристатейный библиографический список

1. Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012. P. 47-390.

2. Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012. P. 391-407.

3. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). Official Journal L 077, 13.03.2004. P. 0001-0011.

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 04.05.2016. P. 1-88.

5. 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.

6. 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.

7. 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 L218, 14.08.2013. P. 8-14.

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

9. Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. OJ L 328, 06.12.2008. P. 55—58.

10. Cyber Security Strategy of the European Union: An open, safe and secure cyberspace. Joint communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, /* JOIN/2013/01 final */•

11. Lietuvos Respublikosbaudziamojo kodekso (https://e-seimas.lrs.lt/ portal/legalAct/lt/TAD/TAIS.111555, свободный (загл. с экрана)).

12. Codepenal (https://www.legifrance.gouv.fr/affichCode.do; jsession id=F06BB691FF16DDFE9DF58E6822AEA8B9.tpdilallv_l?idSectionTA=LEGISCTA000006149817&cidTexte=LEGITEXT000006070719&dat eTexte=20170331, свободный (загл. с экрана)).

13. *Tony Bunyan.* Trevi. Europoland the Europeanstate (http://www. statewatch.org/news/handbook-trevi.pdf, свободный (загл. с экрана)).

14. 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)).

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

16. Digital Single Market // official site of European Commission (https://ec.europa.eu/digital-single-market/en/digital-single-market (загл. с экрана)).

17. About // EuropeanCybercrimeCentre (https://www.europol.europa. eu/about-europol/european-cybercrime-centre-ec3 (загл. с экрана)).

Дело ФАС России в отношении практик Google в сфере операционной системы Android: правовые проблемы и значение для российского антимонопольного регулирования (Москва, Россия)

Е.С. Хохлов[18],[19]

Аннотация. *В настоящей статье рассматриваются правовые и иные аспекты антимонопольного дела в отношении Google, рассмотренного ФАС России. Данное дело касалось различных практик, применявшихся Google в рамках операционной системы Android и магазина Google Play. В статье подробно анализируются фактические обстоятельства , ставшие предметом оценки ФАС России, правовые и иные проблемы, стоявшие перед ФАС России в рамках рассмотрения дела, выводы ФАС России, а также контраргументы, заявлявшиеся Google. Особое внимание уделено проблемам в применении антимонопольного законодательства в отношении интернет-сервисов и отношений по использованию объектов интеллектуальной собственности.*

Ключевые слова: *Федеральная антимонопольная служба, антимонопольное законодательство, злоупотребление доминирующим положением, исключительные права.*

Дело против *Google*[20], рассмотренное Федеральной антимонопольной службой России (далее – ФАС России), является знаковым как для российского антимонопольного регулирования, так и для международного сообщества. ФАС России стала первым антимонопольным органом в мире, давшим негативную оценку практикам *Google* в отношении операционной системы *Android.*

В настоящее время дела в отношении аналогичных фактов рассматриваются Европейской комиссией, Комиссией по справедливой торговле Южной Кореи и с совсем недавнего времени – антимонопольным органом Турции. Европейская комиссия, хронологически уже после принятого ФАС России решения, вынесла свое заключение об обстоятельствах *(statement of objections)*[21] в апреле 2016 г. При этом из пресс-релиза Комиссии, сопровождавшего вынесение заключения об обстоятельствах[22], можно резюмировать, что предварительные выводы Комиссии в целом соответствуют заключениям, к которым пришла ФАС России.

---

[18] Автор являлся частью команды консультантов, представлявшей интересы заявителя в данном деле, – компании Яндекс. В то же время автор, будучи также преподавателем конкурентного права, пытался дать научную оценку сделанным ФАС России выводам.

[19] Следует также сделать важную оговорку: в настоящей статье рассмотрены исключительно вопросы, раскрытые в составе публичного решения и предписания ФАС России. Само дело в ФАС России рассматривалось в закрытом режиме для целей сохранения коммерческой тайны сторон, равно как и последующие судебные разбирательства по данному делу, рассматривавшиеся в закрытых судебных заседаниях по ходатайству *Google.* Поэтому многие детали данного дела, которые могли бы сделать изложение более понятным и подробным, не приводятся.

[20] Решение и предписание ФАС России были вынесены в отношении двух компаний корпорации *Google Inc.* и компании *Google Ireland Limited.* Для целей настоящей статьи обе компании будут именоваться *«Google».*

[21] Заключение об обстоятельствах в конкурентном праве ЕС представляет собой предварительные выводы Комиссии о наличии нарушения антимонопольных норм в действиях хозяйствующего субъекта. Компания, в отношении которой вынесено заключение об обстоятельствах, имеет возможность ответить на него, опровергая выводы Комиссии, и запросить слушания по делу, если посчитает необходимым. Исходя из публичной информации *Google* уже направила Комиссии свой ответ на заключение об обстоятельствах, но не запросила проведение слушаний.

[22] См.: http://europa.eu/rapid/press-release_IP-16-1492_en.htm

В данном деле перед ФАС России стояли непростые вопросы, связанные с тем, подходят ли классические методы антимонопольного регулирования для новой экономики, основанной на информационных технологиях. Данное дело было вдвойне сложным для ФАС России, поскольку в России аналоги таких знаковых дел, как, например, дела против *Microsoft* в ЕС (дела касательно *Windows Media Player* и *Internet Explorer*), на момент рассмотрения дела против *Google* отсутствовали. ФАС России пришлось фактически с нуля формулировать так называемую теорию перенесения рыночной власти (*leveraging theory of harm),* которая является основой обвинения против *Google* в деле по *Android.*

По мнению автора настоящей статьи, подходы классического антимонопольного регулирования вполне применимы в отношении подобных дел, и эта точка зрения в целом разделяется европейскими специалистами. Очевидно, что это не единственная точка зрения, и находятся те, кто полагает, что рынки в сфере информационных технологий обладают такой спецификой, которая требует выработки принципиально новых подходов к их антимонопольному регулированию (а, возможно, и вообще к неприменению мер антимонопольного регулирования к ним).

В частности, сторонники такой точки зрения исходят из того, что многие информационные компании можно слишком легко признать монополистами просто в силу их размера и наличия у них особого положения как владельцев соответствующих информационных платформ (т.е. в силу самого факта обладания такими платформами), что является слишком низким стандартом доказывания. Более того, по мнению данных ученых, на рынках в сфере высоких технологий в принципе невозможно обладание рыночной властью, поскольку «новый лидер рынка может образоваться не только из стартапа, но и путем репозиционирования существующего онлайн-сервиса на смежные рынки»[23], т.е. барьеры доступа на рынок являются низкими.

Представляется, что это упрощенный взгляд на вещи, поскольку сторонники применения традиционного антитраста не отрицают возможности конкуренции между платформами, и в таком случае вывод о наличии доминирующего положения владельца одной из платформ вполне может и не быть сделан. Однако если сама платформа *действительно* является доминирующей (как та же операционная система *Android*), то почему антимонопольные органы не должны пытаться применять антимонопольное законодательство к действиям владельца этой платформы? Применительно к тому, что барьеры доступа на рынки в сфере высоких технологий являются низкими и что конкуренция на них находится «на расстоянии одного клика» *(competition is one click away* – известное выражение основателей *Google*), это опровергается реальной практикой и длительным отсутствием новых конкурентов на многих имеющих значение рынках в сфере информационных технологий, в том числе тех, которые стали предметом рассмотрения ФАС России в деле *Google.*

С развитием новой цифровой экономики перед специалистами в сфере антимонопольного регулирования встал вопрос: что важнее для экономики – инновации или конкуренция? При этом сторонники приоритета инноваций над конкуренцией почему-то противопоставляют эти ценности, т.е. исключают возможность конкуренции при инновациях. Тем не менее конкуренция и инновации вполне совместимы, поскольку одним из следствий конкуренции является внедрение инноваций[24].

Очевидно, что инновации важны, но в долгосрочной перспективе конкуренция важнее, поскольку жизненный цикл той или иной инновации рано или поздно проходит и хозяйствующие субъекты могут начать применять ограничительные практики во вред тем конкурентам,

---

[23] *D. O'Connor.* 'Understanding Online Platform Competition: Common Misunderstandings'. *Internet Competition and Regulation of Online Platforms* (May 2016) // Competition Policy International. P. 9—10.

[24] Подробнее см.: *Сушкевич А.Г.* Институты конкурентного права и новая экономика: как добиться соответствия // Законы России: опыт, анализ, практика. 2016. № 3. С. 21-34.

которые могут дальше развивать инновации в соответствующей области. В связи с этим, по мнению автора настоящей статьи, не должно быть препятствий для применения мер антимонопольного регулирования, если действия обладателя платформы начинают тормозить инновации посредством вытеснения с нее конкурентов.

Решение ФАС России против *Google* вызвало дискуссии в российской и иностранной прессе и профессиональных изданиях. Решение ФАС России было проанализировано в контексте проводимого в ЕС расследования в статье, написанной известными в мире специалистами в области конкурентного права[25], и в данной работе была дана позитивная оценка принятого ФАС России решения против *Google.*

Автор настоящей статьи ставит задачу проанализировать дело ФАС России против *Google* в контексте тех сложностей, которые возникли перед ФАС России при его рассмотрении, а также его значения для российского и международного антимонопольного сообщества.

[25] См.: *B. Edelman and D. Geradin.* 'Android and competition law: exploring and assessing Google's practices in mobile' [2016] // European Competition Journal. P. 1—36.

Ход рассмотрения дела

Прежде чем переходить непосредственно к анализу рассмотренного ФАС России дела и сделанных в рамках него выводов, следует напомнить то, каким образом происходило собственно рассмотрение дела.

Дело было возбуждено в феврале 2015 г. по жалобе Яндекса – российской поисковой системы и основного конкурента *Google* в России и странах СНГ. Изначально дело было возбуждено по такому составу потенциального нарушения, как недобросовестная конкуренция, которая в наиболее общем виде предполагает обязанность хозяйствующего субъекта конкурировать на рынке, используя честные и добросовестные способы и не используя такие методы, которые заведомо направлены на причинение вреда конкурентам. Через некоторое время после возбуждения дела ФАС России добавила еще одну квалификацию, впоследствии ставшую основой для принятия обвинительного решения, – злоупотребление доминирующим положением.

В такой первоначальной «двойственной» квалификации нет ничего удивительного: ФАС России, очевидно, стремилась по такому сложному делу оставить возможность выбора итоговой квалификации на случай, если проанализированные в рамках дела фактические обстоятельства приведут к выводу о наличии только одного нарушения антимонопольных запретов. С формальной точки зрения также не была исключена и возможность, когда определенные практики могли быть признаны недобросовестной конкуренцией, а остальные – злоупотреблением доминирующим положением. С точки зрения теории конкурентного права недобросовестная конкуренция имеет место там, где отсутствует проявление рыночной власти; если же ограничительная практика является проявлением рыночной власти, ее следует квалифицировать как злоупотребление доминирующим положением. В рамках данного дела ФАС России в итоге пришла к выводу о том, что все действия *Google* явились проявлением рыночной власти, вследствие чего в итоге осталась только квалификация в виде злоупотребления доминирующим положением.

В сентябре 2015 г. ФАС России вынесла обвинительное решение, признав *Google* нарушившей российское антимонопольное законодательство применительно к своим практикам в отношении операционной системы *Android*.

В своем решении ФАС России признала антиконкурентыми следующие практики Google:

1. Предоставление своего доминирующего товара – магазина приложений *Google Play* – исключительно в составе пакета приложений *Google Mobile Services* (далее – CMS), который включает в себя более десятка иных приложений от *Google* для ОС *Android.* Тем самым, в соответствии с выводами ФАС России, *Google* переносила свою рыночную силу в отношении *Google Play* на иные приложения для ОС *Android*, получая возможность предустанавливать их на большом количестве устройств без конкурентной борьбы. В то же время конкуренты *Google* в сфере иных мобильных приложений для ОС *Android* не имели возможности предоставить равноценную замену магазину приложений *Google Play*, чтобы предустановить свои приложения на условиях, сопоставимых с условиями предустановки, имевшимися у *Google.*

2. В дополнение к практике связывания *Google* также требовала от производителей мобильных устройств для ОС *Android* соблюдения дополнительных ограничительных требований: (а) настройки поиска *Google* «по умолчанию» во всех точках доступа к поиску на устройствах, (б) приоритетного размещения иконок приложений *Google* на первом экране устройств и (в) запрета на предустановку приложений конкурентов *Google* (включая те, в отношении которых у *Google* отсутствовали конкурирующие приложения), в том числе обусловленного выплатой соответствующего вознаграждения.

В дополнение к решению ФАС России было также вынесено предписание, в соответствии с которым *Google* была обязана:

1) прекратить нарушение и не допускать его в будущем, а именно:

– не обусловливать предоставление *Google Play* требованием об обязательной предустановке иных приложений, сервисов *Google* (CMS);

– не обусловливать предоставление *Google Play* требованием о размещении иконок приложений *Google* (CMS) на главном экране мобильного устройства;

– не обусловливать предоставление *Google Play* требованием о предустановке поисковой системы *Google* в качестве поиска «по умолчанию»;

– не запрещать производителям мобильных устройств предустановку приложений и сервисов конкурентов *Google* (в том числе путем выплаты вознаграждения за отказ вендоров от предустановки приложений и сервисов конкурентов *Google*);

2) совершить все действия, необходимые для внесения изменений во все действующие соглашения/договоры с производителями мобильных устройств с целью исключения из них вышеуказанных требований;

3) проинформировать пользователей мобильных устройств о возможности деактивации предустановленных приложений *Google*, изменения поисковой машины в браузере *Google Chrome*, о возможности установки иного виджета поиска и установки иных приложений, аналогичных входящим в пакет *GMS,* а также о возможности изменения расположения иконок на экране устройства в форме уведомления, которое должно быть выведено на экран мобильного устройства.

Позднее ФАС России наложила на *Google* штраф в размере около 440 млн руб. за злоупотребление доминирующим положением в соответствии со ст. 14.31 КоАП РФ.

Google оспорила решение и предписание ФАС России, а также административный штраф в судебном порядке. В рамках данного судебного разбирательства были приняты решения судов первой и апелляционной инстанций, подтвердившие законность решения и предписания ФАС России.

В связи с имевшимся, по мнению ФАС России, неисполнением предписания было возбуждено соответствующее дело об административном правонарушении, и в конце 2016 г. было принято решение о наложении на *Google* административного штрафа за неисполнение предписания по ст. 19.5 КоАП РФ. *Google* оспорила и этот штраф, и в настоящее время принято решение суда апелляционной инстанции, подтвердившее законность позиции ФАС России.

Но этими процессами дело в отношении *Google* не исчерпывается. ФАС России, полагая свое предписание неисполненным, подала в Арбитражный суд г. Москвы уже собственный иск о понуждении *Google* к исполнению предписания. В свою очередь, *Google* подала еще одно заявление к ФАС России в отношении слишком короткого, по мнению *Google*, срока исполнения предписания, который ФАС России вновь назначила на основании ч. 7 ст. 51 ФЗ от 26.07.2006 № 135-ФЗ «О защите конкуренции» (далее – Закон о защите конкуренции) после того, как признала, что *Google* не исполнила предписание в первоначальный срок и привлекла *Google* к административной ответственности за это.

Таким образом, решение и предписание ФАС России «обросли» множеством разнообразных судебных процессов.

На момент написания настоящей статьи в суде кассационной инстанции по основному делу (об оспаривании решения и предписания ФАС России) было утверждено мировое соглашение, которым был урегулирован спор в отношении решения и предписания ФАС России. Содержание мирового соглашения недоступно публично в связи с тем, что сам спор рассматривался в режиме закрытых судебных заседаний. Тем не менее с существенными условиями

мирового соглашения можно ознакомиться в пресс-релизе ФАС России[26]. Из публикаций в прессе можно сделать вывод о том, что остальные споры между ФАС России и *Google* будут тем или иным образом урегулированы в связи с утверждением мирового соглашения по основному делу и *Google* выплатит наложенные на нее штрафы по ст. 14.31 и ст. 19.5 КоАП РФ.

[26] См.: http://fas.gov.ru/press-center/news/detail.html7icH49773

Ключевые проблемы и развилки, стоявшие перед ФАС России, и выработанные ФАС России решения

(1) *Анализ рынка*

ФАС России определила соответствующий рынок, на котором *Google* была признана занимающей доминирующее положение, как рынок предустанавливаемых магазинов приложений для ОС *Android*, локализованных для России. Локализация отсылает к тому, что для каждой страны фактически существует своя собственная версия магазина приложений, которая должна учитывать национальные особенности (например, язык) и соответствовать требованиям национального законодательства. ФАС России было установлено, что лишь малая часть российских пользователей готова использовать магазин приложений, предназначенный для предустановки на мобильные устройства в другой стране. При этом с точки зрения географических границ рынок был определен как глобальный, поскольку товар, будучи воплощенным в программном обеспечении, может перемещаться от производителя к покупателю в любую точку мира с минимальными затратами.

Было признано, что магазин приложений – самостоятельный товар, который имеет особое функциональное назначение и не может быть заменен другими приложениями. В частности, не является товаром-заменителем мобильный браузер, основная функция которого состоит в предоставлении доступа к веб-страницам и через который лишь незначительное количество пользователей реально скачивает приложения (которые в любом случае могут обновляться только через *Google Play).* При этом ФАС России установила, что *Google Play* с технической точки зрения может функционировать отдельно от других приложений из пакета *GMS.* Важное отличие *Google Play* от других приложений *Google* состоит в том, что иные приложения могут быть скачаны пользователем самостоятельно из *Google Play*, тогда как сам *Google Play* в силу коммерческого решения *Google* невозможно получить иначе, кроме как предустановленным на мобильном устройстве.

При определении границ рынка ФАС России основывалась на Порядке проведения анализа состояния конкуренции на товарном рынке[27].

Однако этот акт не устанавливает каких-либо особенностей в отношении анализа рынков в сфере информационных технологий, поэтому ФАС России пришлось вырабатывать подходы самостоятельно.

Одной из проблем, с которой столкнулась ФАС России, было соотношение традиционного понимания рынка и так называемых многосторонних рынков. В случае с *Google* имеется платформа – операционная система *Android*, вокруг которой «вращается» большое количество отдельных продуктов: те же самые магазины приложений, поиск в Интернете, веб-браузеры, приложения для работы с фото и видео и огромное множество других приложений и сервисов, имеющих различную функциональность. В свою очередь, приложения и сервисы связаны с услугами онлайн-рекламы, с помощью которой данные приложения могут монетизироваться. Некоторые приложения, в том числе и сам магазин приложений, предоставляют возможность монетизации от непосредственно самого приложения; например, встроенные покупки или комиссия, взимаемая с разработчиков за размещение приложений в магазине приложений. Наконец, существуют производители мобильных устройств, которые компонуют свои устройства определенными приложениями и сервисами и взаимодействуют с разработчиками приложений, как правило, по модели разделения доходов от предустановленного приложения/сервиса.

[27] Утвержден Приказом ФАС России от 28.04.2010 № 220 (с последующими изменениями).

Все это многообразие рынков тесно взаимосвязано и характеризуется многосторонними косвенными сетевыми эффектами. Косвенным сетевым эффектом в экономической теории признается ситуация, при которой ценность товара для покупателя на одном рынке повышается, если повышается количество покупателей товара на смежном рынке. Например, ценность рекламы в газете (один рынок) повышается с увеличением количества читателей этой газеты (другой рынок). Многосторонние косвенные сетевые эффекты характерны для платформ, объединяющих несколько элементов воедино. Например, ценность рекламы в приложении «Погода» повышается не только, если увеличивается количество пользователей этого приложения, но и если растет количество пользователей операционной системы, для которой это приложение создано, или количество производителей мобильных устройств, которые используют эту операционную систему[28].

Возникает вопрос, следует ли в таком случае считать рынком всю платформу целиком или определять рынок по каждой стороне платформы в отдельности?

Проблема для ФАС России состояла в том, что понятия многосторонних рынков в российском законодательстве нет. Если в некоторых странах вопрос анализа границ рынка не является принципиальным, и в отношении него может быть допущена определенная степень погрешности, то в случае с российским законодательством и судебной практикой неправильное определение границ рынка может стать самостоятельным основанием для оспаривания решения ФАС России.

Поскольку с формальной точки зрения иного варианта не было, ФАС России определила границы рынка в отношении каждой стороны платформы в отдельности. В то же время ФАС России приняла во внимание при определении границ рынка и рыночной власти *Google* сетевые эффекты в качестве барьеров доступа и экспансии, тем самым учтя особенности многосторонних рынков. Иными словами, сильные косвенные сетевые эффекты, имеющиеся на платформе *Android,* были признаны ФАС России в качестве факторов, осложняющих доступ на какую-либо из сторон этой платформы. ФАС России также было учтено, что *Google* является разработчиком и владельцем самой операционной системы *Android.*

Таким образом, ФАС России фактически сделала вывод о том, что конкуренция существует не только между платформами, но и внутри одной платформы. Этот вывод представляется справедливым в отношении операционной системы *Android,* учитывая, что в нее с момента запуска было привлечено множество производителей устройств и разработчиков приложений и сервисов и что она изначально пропагандировала свою открытость.

Также перед ФАС России встал вопрос о том, может ли в принципе являться товаром объект, в отношении которого не установлена цена (магазины приложений для операционной системы *Android* предоставляются для предустановки бесплатно). Классическое определение товара и рыночной власти привязаны к цене, в частности, именно на этом основан широко известный *SSNIP*-тест (называемый в России «тестом гипотетического монополиста»), а также многие иные тесты для определения границ рынка и рыночной власти.

Однако в случае с *Google Play*, во-первых, можно говорить о том, что встречное предоставление за товар уплачивается не в денежной, а иной форме (например, путем необходимости соблюдать определенные требования к предустановке и (или) приобретения возможности получения доли доходов от онлайн-рекламы). Во-вторых, в случае нулевой цены товара в расчет можно принимать возможность снижения качества товара (поскольку качество в дополнение к цене является ключевым фактором конкуренции). Кроме того, в соответствии с формальным определением товара по ст. 4 Закона о защите конкуренции товаром может являться благо, вводимое в оборот любым способом (в случае с *Google Play* – путем его бесплатной

[28] Подробнее о многосторонних сетевых эффектах в контексте дела *Google* см.: *Юсупова Г. Ф.* ФАС против Google: экономический анализ для особых рынков // Экономическая политика. 2016. Т. 11. № 6. С. 82—99.

предустановки). Таким образом, тот факт, что какой-то объект гражданских прав предоставляется условно-бесплатно, не влияет на возможность его квалификации как товара с точки зрения антимонопольного законодательства.

Наконец, ФАС России был проанализирован вопрос о том, могут ли считаться взаимозаменяемыми магазины приложений, разработанные для других операционных систем для мобильных устройств, и был сделан вывод, что не могут. Поскольку операционная система *iOS*, разработанная корпорацией *Apple*, является закрытой системой и не представляется для лицензирования иным производителям мобильных устройств, кроме корпорации *Apple*, производители мобильных устройств в настоящее время имеют выбор между ОС *Android* и ОС *Windows Phone* (доля других операционных систем для мобильных устройств ничтожно мала). При этом переключение на магазин приложений, разработанный под другую операционную систему, невозможно без переключения на другую операционную систему.

ФАС России проанализировала реальную рыночную практику и пришла к выводу, что лишь крайне небольшое количество производителей мобильных устройств фактически производят мобильные устройства для последующей реализации в России на ОС *Windows Phone* или альтернативных операционных системах. Причем наибольшее количество таких устройств производилось компанией *Nokia*, которая контролируется производителем одной из альтернативных операционных систем (ОС *Windows Phone)* – корпорацией *Microsoft.* При этом фактические данные говорят о том, что переключения на другую операционную систему на практике почти не происходят, а те, которые имели место, были коммерчески неуспешны (например, попытка запуска *Samsung* собственной операционной системы *Tizen).*

Помимо сложностей для производителей мобильных устройств, связанных с переключением на другую операционную систему, были учтены и сложности для пользователей. Например, невозможен перенос приобретенных приложений с мобильного устройства, работающего на одной операционной системе, на мобильное устройство, работающее на другой операционной системе. Вследствие этого переход производителя мобильных устройств на другую операционную систему будет означать потерю значительного количества лояльных пользователей, фактически теряющих при смене мобильного устройства ранее приобретенные ими приложения (и сделанные в них встроенные покупки).

(2) *Измерение рыночной власти/определение доминирующего положения*

Как отмечалось выше, вопрос измерения рыночной власти в сфере многосторонних рынков в соответствии с традиционными методами антимонопольного регулирования является непростым, особенно в ситуации, когда товар предоставляется (условно) бесплатно. Тем не менее ФАС России выработала подход, позволивший ей сделать вывод о наличии у *Google* рыночной власти и, следовательно, доминирующего положения.

Google Play – самый популярный и наиболее распространенный магазин приложений на ОС *Android.* ФАС России установила, что если на мобильном устройстве под управлением ОС *Android* отсутствует *Google Play*, такое устройство не будет коммерчески успешным у пользователей, поэтому все основные производители мобильных устройств на ОС *Android* вынуждены обращаться к *Google* за получением *Google Play.*

При этом *Google Play* в принципе предоставляется только производителям мобильных устройств[29]. Конечные пользователи мобильных устройств не имеют возможности самостоятельно загрузить магазин приложений *Google Play* из какого бы то ни было источника, т.е. не могут его использовать, если только он не предустановлен производителем на соответствую-

[29] См.: http://source.android.com/source/faqs.html#if-i-am-not-a-manufacturer-how-can-i-get-google-play

щем мобильном устройстве. Кроме того, с помощью *Google Play* невозможно загрузить магазины приложений иных производителей[30].

ФАС России сделала вывод, что в сфере мобильных приложений и сервисов предустановка – это ключевой способ продвижения товара, обусловливающий коммерческий успех того или иного приложения. Как показали представленные в дело социологические исследования ВЦИОМ и «Ромир», подавляющее большинство пользователей пользуется тем, что предустановлено на устройстве или настроено по умолчанию. Лишь малая их часть загружает приложения самостоятельно (а в отношении *Google Play*, как отмечалось, это в принципе невозможно).

Поэтому ФАС России посчитала, что рыночную власть в рассматриваемом случае можно определить посредством количества устройств, на которых предустановлены магазины приложений (как некий аналог доли рынка в традиционном понимании).

Помимо этого, как отмечалось, ФАС России учла и наличие на рынке сильных косвенных сетевых эффектов, а также были учтены иные барьеры входа/экспансии, в том числе обусловленные собственными действиями/требованиями *Google.*

(3) *Существо злоупотребления доминирующим положением*

Ключевая практика, признанная ФАС России антиконкурентной, – это связывание доминирующего товара (магазина приложений *Google Play)* с иными товарами, которые могут обращаться на конкурентных рынках (отдельными приложениями и сервисами, входящими в состав *GMS).* ФАС России установила, что требование предустановки множества различных по функционалу приложений совместно с *Google Play* не было обусловлено технологическими причинами. Достаточно сказать, что даже если какое-либо из приложений из пакета *GMS* не предустановлено на устройстве, оно может быть самостоятельно загружено пользователем из магазина приложений *Google Play.*

С точки зрения негативных последствий для конкуренции от практики связывания ФАС России применила так называемую теорию перенесения рыночной власти (*leveraging theory*), признав, что *Google* распространила свою рыночную власть применительно к *Google Play* на иные собственные приложения, получая возможность предустановить их на большом количестве устройств бесплатно и без конкурентной борьбы. Путем связывания *Google* повышала для своих конкурентов стоимость конкуренции, что приводило к необходимости последним тратить существенные ресурсы для предустановки своих приложений либо пытаться предложить аналог *Google Play* и всех иных приложений, входящих в *GMS* (что заведомо невыполнимо).

При этом ФАС России учла, что пакетирование само по себе является допустимым способом продвижения товара. ФАС России указала в решении, что само по себе связывание не является нарушением, однако оно становится таковым, если пакетирование применяется доминирующим субъектом в качестве *единственного* способа продвижения своего доминирующего товара (возможность отдельного приобретения которого у покупателя отсутствует)[31]. То есть *Google* была признана злоупотребившей своим доминирующим положением не в силу самого по себе факта связывания, а поскольку у производителей мобильных устройств отсутствовала иная возможность получения *Google Play*, кроме как в составе пакета *GMS.*

Такой вид злоупотребления доминирующим положением, как пакетирование (связывание)[32], является хорошо разработанным в зарубежной антимонопольной практике и литера-

---

[30] См. разд. 4.5 Соглашения *Google Play* о распространении программных продуктов (https://play.google.com/about/deyeloper-distribution-agreement.html).

[31] В экономической теории данный вид связывания получил наименование «чистое связывание» *(pure bundling).*

[32] Понятия «пакетирование» (*bundling*) и «связывание» *(tying),* пришедшие из зарубежного права, в целом совпадают; под ними понимается такое явление, как «продажа в нагрузку», т.е. условием приобретения одного (доминирующего) товара является приобретение другого (недоминирующего) товара или нескольких товаров. Различия состоят в том, что связывание представляет собой неценовую практику, т.е. любую ситуацию, при которой совместное приобретение доминирующего и недо-

туре. Как отмечалось выше, в сфере высоких технологий в ЕС уже имелись прецедентные дела в отношении корпорации *Microsoft* (дела в отношении *Windows Media Player* и *Internet Explorer*), не говоря уже о том, что и до дел в отношении *Microsoft* существовала хорошо проработанная правоприменительная практика в других областях (дела *Hilti, Tetra Pak* и др.).

В отличие от конкурентного права ЕС антимонопольных дел по связыванию в России практически не было. Фактически единственными прецедентами были дела против естественной монополии – РЖД. В одном показательном деле ОАО «РЖД» по умолчанию включало в стоимость билета на пассажирскую перевозку стоимость страховки от несчастных случаев, предоставляемой входящей в его группу страховой компанией. В другом деле ОАО «РЖД» включало в стоимость перевозки пассажиров в плацкартном вагоне стоимость дополнительной услуги – использования постельного белья.

Несмотря на то что связывание как вид злоупотребления доминирующим положением напрямую не предусмотрено ст. 10 Закона о защите конкуренции, закрепленное в данной статье общее понятие злоупотребления дало ФАС России возможность применить концепцию связывания в рассматриваемом деле.

Помимо собственно связывания, ФАС России признала антиконкурентными и иные вытекающие из него практики. В частности, то, что предустановка *Google Play* требовала от производителей мобильных устройств соблюдения дополнительных ограничительных требований *Google*: (1) приоритетного размещения иконок приложений *Google* на первом экране мобильного устройства; (2) настройки поиска *Google* «по умолчанию» во всех точках ввода поискового запроса на мобильном устройстве и (3) запрета на предустановку приложений, разработанных конкурентами *Google.* Данные практики *Google* были признаны ФАС России повлекшими ограничение конкуренции и нарушение интересов конкурентов *Google*, являющихся разработчиками мобильных приложений и сервисов, что выразилось в первую очередь в прямых отказах производителей мобильных устройств предустанавливать мобильные приложения конкурентов *Google.*

В частности, условие о приоритетном размещении мобильных приложений на экране мобильного устройства ограничивало возможность конкурентов договариваться с производителями о размещении своих приложений на условиях, аналогичных тем, на которых предустанавливались приложения *Google.* Приоритетное размещение на экране обеспечивает более высокую частоту использования приложений по сравнению с теми приложениями, которые размещены на менее выгодных местах на экране. Условия о настройке поиска *Google* в качестве поиска, по умолчанию, во *всех* точках доступа на устройстве и о запрете предустановки приложений конкурентов имеют непосредственный вытесняющий эффект (представляют собой «прямое исключение» *(naked exclusion)).*

В итоге ФАС Росси пришла к выводу о том, что *Google* получала преимущество перед конкурентами не за счет конкурентной борьбы, а исключительно за счет своей рыночной власти в отношении *Google Play.*

(4) *Исключение для осуществления исключительных прав в отношении объектов интеллектуальной собственности*

В ч. 4 ст. 10 Закона о защите конкуренции содержится исключение для действий доминирующих субъектов, сформулированное следующим образом: «Требования настоящей статьи

минирующего товара делается вынужденным или выгодным с использованием неценовых методов (через соответствующие требования в договорах, отказ в поставке доминирующего товара, технические особенности, делающие затруднительным или невозможным приобретение товаров по отдельности). Пакетирование представляет собой практику, при которой несколько товаров реализуется единовременно по единой цене. Несмотря на различия, антиконкурентный эффект у данных практик является одинаковым, более того, зачастую ценовые и неценовые факторы, способствующие практике пакетирования (связывания), используются доминирующими субъектами в совокупности. Поэтому для целей настоящей статьи данные понятия используются как синонимы.

(запреты для доминирующих субъектов. – *Е.Х.)* не распространяются на действия по осуществлению исключительных прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, средства индивидуализации продукции, работ или услуг».

Очевидно, что в рамках рассмотрения дела *Google* ссылалась на данное исключение в обоснование правомерности своих практик.

В частности, *Google* занимала позицию о том, что все ее действия, признанные злоупотреблением доминирующим положением, были действиями по осуществлению исключительных прав на результаты интеллектуальной деятельности (к которым относится собственно магазин приложений *Google Play* как программа для ЭВМ), а заключаемые с производителями мобильных устройств соглашения являлись лицензионными[33]. Кроме того, поскольку данные соглашения подчинены иностранному, а не российскому праву, то и понятие осуществления исключительных прав должно толковаться в соответствии с иностранным правом.

ФАС России, в том числе с учетом правовых заключений, подготовленных Московским государственным юридическим университетом им. О.Е. Кутафина (МГЮА) (проф. М.А. Рожкова) и Институтом законодательства и сравнительного правоведения (доц. В.О. Калятин), пришла к выводу о том, что спорные действия *Google* выходят за пределы осуществления его исключительных прав, и, следовательно, к ним не подлежит применению исключение, предусмотренное ч. 4 ст. 10 Закона о защите конкуренции. ФАС России также сочла необходимым толковать понятие «осуществление исключительных прав» в соответствии с российским, а не иностранным правом.

Аргументация ФАС России состояла в следующем. Исключение по ч. 4 ст. 10 Закона о защите конкуренции означает, что обладателя исключительного права на определенный результат интеллектуальной деятельности нельзя признать лицом, занимающим доминирующее положение, исключительно в силу наличия такого исключительного права, а действия по распоряжению своим исключительным правом, в том числе путем заключения лицензионного договора, не подпадают под антимонопольные запреты.

Однако это не означает, что вообще любые положения (ограничительные условия), содержащиеся в договоре, в рамках которого осуществляется передача лицензии, являются автоматически относящимися к лицензионным правоотношениям и не подлежат оценке в соответствии с антимонопольным законодательством.

Осуществлением исключительного права является реализация заложенных в соответствующем субъективном праве возможностей в предусмотренных законом пределах. В соответствии с п. 1 ст. 1229 ГК РФ правообладатель наделен правом использовать результат интеллектуальной деятельности по своему усмотрению любым не противоречащим закону способом, распоряжаться исключительных правом (в частности, путем отчуждения в полном объеме или предоставления права использования третьем улицу), а также по своему усмотрению разрешать или запрещать другим лицам использование результата интеллектуальной деятельности. При этом ограничительные требования *Google* при предоставлении магазина приложений *Google Play* подлежат оценке только с точки зрения правомочия распоряжения исключительным правом, поскольку *Google* предоставляла магазин приложений для его использования (предустановки) третьим лицам.

В соответствии с закрепленным в российском праве подходом лицензионное правоотношение представляет собой предоставление одним лицом (правообладателем) другому лицу

---

[33] Сами положения договоров, заключаемых *Google* с производителями мобильных устройств на *Android*, являются конфиденциальными. Тем не менее публично доступны два договора о продвижении мобильных приложений *Google (Mobile Application Distribution Agreements*), заключенные *Google* с *Samsung* и *HTC* в редакции 2011 г., которые были раскрыты в рамках разбирательства по делу *Oracle America* v. *Google* в США. Дальнейшие отсылки к договору *MAD A* сделаны на публично доступные тексты договоров.

(лицензиату) права использования объекта исключительных прав на определенный срок, в рамках согласованной территории и в пределах тех способов использования, которые возможны для соответствующего объекта в силу его природы, а также допустимы в соответствии с российским законодательством.

В частности, в отношении программ для ЭВМ (к которым относится *Google Play)* перечень способов использования приведен в п. 2 ст. 1270 ГК РФ (например, воспроизведение, доведение до всеобщего сведения и пр.). Указанный перечень не является закрытым, использование объекта интеллектуальных прав возможно и другими способами, однако все они подразумевают совершение определенных операций либо с программой для ЭВМ (например, создание копий), либо с материальным носителем, содержащим такую программу (например, продажа носителя). Указание на «предусмотренные договором пределы» следует понимать в значении поди. 2 и. 6 ст. 1235 ГК РФ как согласование в договоре конкретных способов использования результата интеллектуальной деятельности, а также территории и срока, в пределах которых такое использование разрешается.

Однако соглашения с *Google* имели более широкий предмет, нежели простое предоставление лицензии на приложения из состава *GMS;* основным элементом соглашений являлись обязательства производителей мобильных устройств по продвижению приложений и сервисов *Google* для мобильных устройств. Иными словами, предмет соглашений *Google* был шире, чем предоставление лицензии. Даже из самого наименования договоров, которые *Google* заключала с производителями мобильных устройств, можно сделать вывод о том, что они носили смешанный характер и не могли квалифицироваться как обычный лицензионный договор. Так, договор *MAD A* («Договор дистрибуции мобильных приложений») в своем наименовании содержит указание на обязательство производителей по продвижению мобильных приложений, а вовсе не на предоставление им права использования результатов интеллектуальной деятельности.

Исходя из вышеизложенного ФАС России пришла к выводу о том, что соглашения *Google* являются смешанными, а элемент предоставления лицензии – вспомогательным (необходим для того, чтобы производители мобильных устройств могли осуществить свою основную обязанность по продвижению приложений и сервисов *Google).* При этом ограничительные условия, признанные ФАС России злоупотреблением доминирующим положением (в частности, запрет предустановки приложений и сервисов конкурентов, требование о преимущественном размещении приложений и сервисов *Google*, требование о настройке поиска *Google* в качестве единственного поиска по умолчанию на устройствах), относились именно к основному предмету соглашений – продвижению приложений и сервисов *Google.* ФАС России сделала вывод о том, что запреты и ограничения *Google* являлись самостоятельными обязательствами – требованиями к дистрибуции мобильных приложений, сходными по своему характеру с обязательствами об оказании услуг. Поскольку данные ограничительные требования не входят в состав лицензионных правоотношений, они были признаны не подпадающими под исключение по ч. 4 ст. 10 Закона о защите конкуренции.

Применительно к самой практике связывания обязанность использовать все программы для ЭВМ исключительно совместно также была признана выходящей за пределы осуществления исключительных прав на каждую из программ для ЭВМ, входящую в пакет. Требование об использовании одного результата интеллектуальной деятельности (РИД 1) только при одновременном использовании другого результата интеллектуальной деятельности (РИД 2) не является элементом осуществления исключительного права на РИД 1, поскольку никак не касается определения способов и пределов использования РИД 1.

ФАС России в этой связи указала: «Самостоятельным объектом исключительных прав является каждая конкретная программа для ЭВМ (приложение), осуществление исключительных прав на которые охватывает только действия по использованию данной программы, но не весь процесс коммерческой деятельности, связанный с ним. Соответственно в предмет дого-

вора, оформляющего предоставление права использования программы для ЭВМ, может включаться только описание пределов использования программы. Любые иные вопросы взаимоотношений сторон, которые также может урегулировать лицензионный договор, будут выходить за пределы лицензионных правоотношений».

Правомерность позиции ФАС России подтверждается имеющейся судебной практикой. В частности, по делу *Ангстрем* (дело № А40-3954/10-149-52) Президиум ВАС РФ в Постановлении от 29.11.2011 № 6577/11 поддержал доводы кассационной инстанции о том, что не подпадает под исключение по ч. 4 ст. 10 Закона о защите конкуренции условие об эксклюзивности в лицензионном договоре, не касающееся непосредственно права на использование результата интеллектуальной деятельности. Аналогичная позиция была сформулирована кассационной инстанцией по знаковому делу *Teva* (дело № А40-42997/2014) и впоследствии поддержана ВС РФ.

Применительно к аргументу *Google* о том, что понятие «осуществление исключительных прав» должно толковаться в соответствии с иностранным правом, которому подчинены соглашения *Google* с производителями мобильных устройств, ФАС России заняла следующую позицию.

В соответствии с и. 2 ст. 1231 ГК РФ при признании исключительного права на результат интеллектуальной деятельности или средство индивидуализации в соответствии с международным договором Российской Федерации содержание права, его действие, ограничения, порядок его осуществления и защиты определяются ГК РФ независимо от положений законодательства страны возникновения исключительного права, если таким международным договором или ГК РФ не предусмотрено иное.

Иными словами, если иностранные лица заключают соглашение об использовании результата интеллектуальной деятельности и подчиняют его иностранному праву, то к их договорным отношениям действительно будет применяться иностранное право, однако это никак не повлияет на применение российского права к объему и порядку осуществления права на такой результат интеллектуальной деятельности на территории России. Стороны не могут, подчинив договор иностранному праву, предусмотреть, что объем предоставленного права использования программы для ЭВМ в России будет определяться этим иностранным правом, поскольку само по себе предоставление права использования на территории России оказывается возможным исключительно в силу того, что на основании указанного выше положения ГК РФ право на программы для ЭВМ, созданные за рубежом, признаются в России и объем такого права определяется именно правом России.

Кроме того, при применении исключения, предусмотренного ч. 4 ст. 10 Закона о защите конкуренции, ФАС России основывалась на понятии «осуществление исключительных прав» согласно российскому праву, поскольку данное исключение содержится именно в *российском* законодательстве. В связи с тем, что Закон о защите конкуренции основан на ГК РФ (см. ч. 1 ст. 2 Закона о защите конкуренции), понятие «осуществление исключительных прав» для целей оценки применимости ч. 4 ст. 10 Закона о защите конкуренции подлежит толкованию в соответствии с ГК РФ, несмотря на то, что договор в отношении того или иного объекта интеллектуальной собственности может быть подчинен иностранному праву.

* * *

В данном деле были также затронуты многочисленные иные юридические и экономические вопросы, которые сделали это дело беспрецедентным (по крайней мере в российской практике) по сложности и многоаспектности. Как отмечалось, закрытый характер рассмотрения этого дела препятствует анализу всех вопросов в необходимых для этого подробностях. Тем не менее представляется, что даже вышеизложенное позволяет сделать вывод о том, что

ФАС России смогла разобраться в крайне сложной индустрии информационных технологий и применить к ней традиционные методы антимонопольного регулирования без ущерба для высоких стандартов доказывания, принятых в ЕС и других ведущих мировых юрисдикциях.

Пристатейный библиографический список

1. *Юсупова Г.Ф.* ФАС против Google: экономический анализ для особых рынков // Экономическая политика. 2016. Т. 11. № 6. С. 82— 99.

2. *B. Edelman and D. Geradin.* 'Android and competition law: exploring and assessing Google's practices in mobile' [2016] // European Competition Journal. P. 1-36.

3. *D. O'Connor*: 'Understanding Online Platform Competition: Common Misunderstandings', *Internet Competition and Regulation of Online Platforms* (May 2016) // Competition Policy International. P. 9-10.

Право на защиту персональных данных и различные категории персональных данных (Москва, Россия)

Б.С. Бембеева

Аннотация. *В практике Европейского суда по правам человека защита персональных данных рассматривается как часть права на неприкосновенность частной жизни, которое гарантировано ст. 8 Конвенции по правам человека. В статье анализируется практика по делам, в которых категории персональных данных можно разграничить в зависимости от источника информации.*

Ключевые слова: *персональные данные, право на неприкосновенность частной жизни, Европейский Суд по правам человека.*

В 1890 г. судьями Верховного суда США Льюисом Брандейсом и Сэмюэлем Уорреном была опубликована статья «Право на частную жизнь» (*The Right to Privacy*), в которой впервые был использован термин *privacy*[34]. Изначально данный термин трактовался американскими судьями как свобода личности от вмешательства государства. Они подразумевали под этим право на автономность (*the right to be let alone)* и использовали его преимущественно в пространственном аспекте[35]. Необходимо отметить, что право на автономность отождествлялось с правом на жизнь и правом на защиту собственности: *«The right to life has come to mean the right to enjoy life, – the right to be let alone»*[36]. Но сегодня право на уважение частной жизни является отдельной категорией, которая не ограничивается только личным пространством, а включает в себя и информационную «среду обитания» человека.

Стоит отметить, что с одной стороны, глобализация, научно-техническое развитие, информатизация общества создают условия для дальнейшего развития индивида как личности, для полноценной и эффективной реализации его прав и свобод. С другой стороны, происходящие изменения способствуют созданию предпосылок для нарушения права человека на уважение частной жизни. В частности, в ст. 11 Венской декларации и Программы действий отмечается, что прогресс в области информационных технологий может иметь потенциально негативные последствия для неприкосновенности, достоинства и прав человеческой личности[37]. Это связано с тем, что современные технологии способствуют расширению возможностей обработки и распространения информации, что в значительной степени обостряет проблему неприкосновенности частной жизни человека и вмешательства в нее со стороны государства.

Как отмечалось в докладе Управления Верховного комиссара ООН по правам человека, во многих государствах практика указывает на отсутствие надлежащего национального законодательства, слабые процедурные гарантии и неэффективный надзор, что в совокупности приводит к отсутствию ответственности за произвольное или незаконное вмешательство в частную жизнь человека со стороны государства[38].

---

[34] *Samuel D. Warren, Louis D. Brandeis.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4, No. 5. P. 193.

[35] *Глинская Н.П.* Юридический термин *privacy* как предмет системно-динамического исследования // Вестник Московского университета. Серия 19: Лингвистика и межкультурная коммуникация. 2010. № 2. С. 36.

[36] *Samuel D. Warren, Louis D. Brandeis.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4, No. 5. P. 193.

[37] Всемирная конференция по правам человека. Венская декларация и Программа действий. Июнь 1993 г. Нью-Йорк: Организация Объединенных Наций, 1995. С. 21—60.

[38] Управление Верховного комиссара ООН по правам человека (УВКПЧ) URL: http:// webcache.googleusercontent.com/search?q=cache:V9hn01GUwToJ:www.ohchr.org/EN/ H R Bodies/H RC/RegularSessions/Session27/Documents/A- H

Вместе с тем нельзя не замечать, что защищаемые права, существующие вне цифровой среды, постепенно получают правовую регламентацию. Тогда как по-иному ситуация обстоит с правами на неприкосновенность частной жизни, связанными с цифровым пространством, и прежде всего правом на защиту персональных данных. Право на защиту персональных данных не закреплено в международно-правовых актах как самостоятельное и обычно рассматривается как один из аспектов защиты частной жизни, формируясь под воздействием судебной практики международных судов.

Значительное влияние на развитие международного и национального законодательства в области защиты персональных данных оказывает ЕСПЧ. Практика ЕСПЧ развивает современное представление о правах человека и устанавливает стандарты их обеспечения и защиты: «Практику ЕСПЧ, в ходе которой вырабатываются правовые позиции Суда, характеризует привнесение в современное научно-технологическое развитие фундаментальных ограничителей, что позволяет осуществить баланс между интересами научно-технологического развития и интересами человека»[39].

В этих условиях несомненный интерес представляет прецедентная практика ЕСПЧ по толкованию норм, содержащихся в ст. 8 Конвенции по правам человека, которая закрепляет право на уважение частной и семейной жизни: «1. Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.

2. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц».

Анализ практики ЕСПЧ позволил выделить несколько категорий персональных данных, вопрос о защите которых не раз ставился перед Судом. Предварить обзор о разновидностях персональных данных необходимо ссылкой на Конвенцию о защите физических лиц при автоматизированной обработке персональных данных 1981 г. (далее – Конвенция о персональных данных), согласно которой под персональными данными следует понимать «любую информацию об определенном или поддающемся определению физическом лице»[40].

RC-27-37_en.doc+&cd= 1 &hl= ru&ct=clnk&gl=ru (дата обращения: 28.03.17).

[39] *Шугуров М.В.* Защита прав человека в условиях современного научно-технического прогресса: практика Европейского суда по правам человека // Международное публичное и частное право. 2011. № 1. С. 5.

[40] Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 // Бюллетень международных договоров. 2014. № 4.

ДНК и отпечатки пальцев

Эти биометрические данные признаются неповторимым и особенным источником данных о человеке. Осуществление незаконного сбора и хранения таких данных, безусловно, противоречит ст. 8 Конвенции по правам человека. И здесь следует обратить внимание на то, что Рекомендация Совета Европы № R(87)15, регламентирующая вопросы использования информации персонального характера в ходе деятельности полиции, допускает возможность хранения подобной информации с определенными ограничениями. В частности, предусмотрена обязанность принимать все необходимые меры, чтобы информация личного характера, хранящаяся для целей деятельности полиции, удалялась, если в ней отпадает объективная необходимость[41].

Принцип необходимости хранения информации личного характера в зависимости от преследуемых целей нашел отражение в нескольких решениях ЕСПЧ.

В деле «*S. и Марпер против Соединенного Королевства*»[42] ЕСПЧ, ссылаясь на ст. 7 Конвенции о персональных данных, напомнил, что национальное законодательство государств – участников Конвенции должно предусматривать достаточные гарантии эффективной защиты хранящихся персональных данных от ненадлежащего использования и злоупотреблений.

Заявители по этому делу обвинялись в совершении уголовных преступлений, но впоследствии были оправданы национальным судом. Во время расследования этих преступлений у обвиняемых были сняты образцы отпечатков пальцев, взяты анализы ДНК, а также образцы их клеток. После прекращения уголовного преследования в отношении обоих заявителей они обратились к полиции с требованием уничтожить взятые биологические материалы из национальной базы данных (в которой подобная информация хранилась бессрочно). Но полиция отказалась это сделать, ссылаясь на ст. 64 Акта о полиции и доказательствах по уголовным делам 1984 г., согласно которой отпечатки пальцев или образцы ДНК могли храниться после того, как они были использованы для достижения цели, ради которой они были взяты[43].

ЕСПЧ поддержал позицию заявителей, отметив, что хранение отпечатков пальцев и ДНК по делам, в которых обвиняемые по уголовным делам были оправданы или их уголовное преследование было прекращено, является нарушением ст. 8 Конвенции по правам человека. Ссылаясь на решение по делу *«Леандер против Швеции»*[44], ЕСПЧ отметил, что даже простое хранение информации, относящейся к личной жизни человека, является вмешательством государства в осуществление его прав по смыслу положений ст. 8 Конвенции по правам человека. По мнению ЕСПЧ, профили ДНК предоставляют государству необходимые средства для установления генетических связей между большим количеством людей, что само по себе достаточно для вывода о том, что их хранение представляет собой вмешательство государства в осуществление этими людьми права на неприкосновенность их личной жизни[45]. Что касается отпечатков пальцев, то Суд подчеркнул, что они объективно содержат уникальную информацию о человеке, а в ряде случаев позволяют точно идентифицировать его личность. Таким образом, это может негативно отразиться на неприкосновенности частной жизни, а хра-

---

[41] Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector // OSCE POLIS URL: https://goo.gl/qiz6Ey (дата обращения: 15.04.2017).

[42] S. and Marper y. The United Kingdom, постановление от 04.12.2008, жалобы № 30562/04 и № 30566/04.

[43] Примечательно, что в более ранней редакции этого акта закона возможность уничтожения подобных данных осуществлялась при первой же возможности после окончания производства по делу.

[44] Leander y. Sweden, постановление от 27.03.1987, жалоба № 9248/81. § 48.

[45] *S. and Marper* v. The United Kingdom, постановление от 04Л2.2008, жалобы № 30562/04 и № 30566/04, § 75.

нение подобной информации без согласия лица, которому она принадлежит, нельзя назвать нейтральным или незначительным[46].

При этом ЕСПЧ не отрицает того, что в некоторых случаях вмешательство в право заявителя на неприкосновенность частной жизни может быть признано законным. Но это допустимо лишь при соблюдении некоторых условий, на которые Суд специально обращает внимание.

Так, заявитель по делу *«Ван дер Вельден против Нидерландов»*[47] обвинялся в вымогательстве и содержался в одном из исправительных учреждений г. Дордрехта на основании медицинских заключений сразу нескольких врачей, которые отмечали высокий риск возможности рецидива у заявителя. Государственный прокурор на основании национального законодательства – ст. 2 § 1 Закона о взятии анализа ДНК улиц, осужденных за уголовные преступления, издал приказ об отборе клеточного материала для определения ДНК-профиля заявителя.

По мнению заявителя, приказ государственного прокурора об отборе у него клеточного материала и хранение полученного образца ДНК-профиля в государственной базе данных, по сути, повлек для него дополнительное наказание по смыслу ст. 7 Конвенции по правам человека, поскольку он уже содержался в исправительном учреждении. Он также обратил внимание на то, что вопрос о его ДНК-профиле вовсе не поднимался во время непосредственного проведения расследования уголовного преступления, что указывало на применение дискриминационных мер в отношении него. Это и стало основанием для обращения в ЕСПЧ с жалобой на нарушение ст. 8 и 14 Конвенции по правам человека.

ЕСПЧ признал эту жалобу неприемлемой. При этом Суд отметил, что в данном случае хранение ДНК не являлось вмешательством в частную жизнь, так как это было предусмотрено законом, преследовало правомерные цели предупреждения преступлений и защиты прав и свобод других лиц. Кроме того, по мнению ЕСПЧ, рассматриваемое вмешательство было сравнительно незначительным. В своем решении о неприемлемости этой жалобы ЕСПЧ отметил несомненную пользу, принесенную базой ДНК-профилей в сфере обеспечения правопорядка за последние годы. Также Суд указал, что заявитель может извлечь и некоторую выгоду из включения его ДНК-профиля в национальную базу данных, учитывая высокий риск рецидива: в будущем он может быть быстро исключен из списка лиц, подозреваемых в совершении преступлений, что осуществимо путем сравнения его биометрических данных с другими полученными образцами.

[46] Там же. § 84.

[47] Van der Velden v. Netherlands, решение по вопросу приемлемости жалобы от 07.12. 2006 по делу жалоба № 29514/05.

Образцы голоса, полученные с помощью прослушивающих устройств

Правовая регламентация использования такой категории информации о человеке, как голосовые данные, составляет одну их проблемных частей в законодательстве многих государств. Вследствие этого на рассмотрение ЕСПЧ передавались дела, связанные со сбором этих персональных данных в ходе оперативно-розыскных мероприятий.

В деле *«P.G. and J.H. против Соединенного Королевства»*[48] устройства секретного прослушивания были установлены в квартире одного из заявителей. Заявители подозревались в подготовке вооруженного ограбления и были задержаны полицией уже после установки прослушивающих устройств. В полицейском участке их допрос был также записан на скрытое прослушивающее устройство, а полученные образцы голосов были отправлены эксперту, который подтвердил их схожесть с образцами голосовых данных, полученных путем секретного прослушивания в квартире.

Заявители обратились с жалобой в ЕСПЧ, указывая на нарушения ст. 6, 8 и 13 Конвенции по правам человека действиями национальных властей при проведении расследования. Заявители, отвечая на вопросы полицейских в участке, не могли знать, что их голос записывается с целью сравнения полученных данных с уже записанными образцами. Полученные голосовые данные впоследствии использовались полицией в суде в качестве доказательств совершения ими уголовного преступления. И, по сути, сам факт того, что заявители отвечали на вопросы полицейских, в данном случае стало свидетельствованием их против самих себя.

В свою очередь, государство-ответчик утверждало, что использование прослушивающих устройств не влечет каких-либо нарушений Конвенции, поскольку эти записи не были сделаны для получения информации непосредственно о частной жизни заявителей. По мнению правительства, записи, сделанные во время допроса заявителей, представляли собой часть формального процесса уголовного правосудия и осуществлялись в присутствии по крайней мере одного офицера полиции[49].

ЕСПЧ пришел к выводу, что установка прослушивающих устройств в квартире и секретная запись допроса на диктофон представляют собой нарушение ст. 8 Конвенции по правам человека. При этом Суд отметил, что в соответствующее время в правовой системе государства-ответчика не существовало законодательного акта, который регулировал использование скрытых подслушивающих устройств полицией в их собственных помещениях. Запись и анализ их голосов по этому поводу все равно должны рассматриваться как обработка персональных данных о заявителях. В связи с этим Суд сделал вывод о том, что в данном случае имело место вмешательство государства в частную жизнь заявителя, что является нарушением ст. 8 Конвенции по правам человека.

В деле *«Веттер против Франции»*[50] заявитель обвинялся в совершении убийства и был приговорен к 20 годам тюрьмы. Обвинения против него основывались на данных, полученных полицией путем установки прослушивающих устройств в квартире жертвы, которую регулярно посещал заявитель.

---

[48] *P.G. and J.H. v. The United Kingdom*, постановление от 25.09.2001, жалоба № 44787/98.

[49] При этом необходимо отметить, что добровольность дачи показаний, по мнению ЕСПЧ, не распространяется на получение документов и образцов биологического происхождения у живого человека (см. подробнее: Saunders v. The United Kingdom, постановление от 17.12.1996, жалоба № 19187/91).

[50] *Vetter* v. *France*, постановление от 31.05.2005, жалоба № 59842/00.

ЕСПЧ при рассмотрении этого дела отметил, что национальное законодательство Франции хотя и содержит некоторые положения о перехвате телефонных разговоров, но не регламентирует порядок

установления прослушивающих устройств. В частности, во французском законодательстве не уточняется свобода усмотрения государства в отношении использования прослушивающих устройств, а также процедура, с помощью которой должно осуществляться использование полученных голосовых данных в целях расследования преступлений. Исходя из этого ЕСПЧ признал, что в этом деле имело место нарушение ст. 8 Конвенции по правам человека.

Данные, полученные с помощью системы глобального позиционирования (GPS)

Нарушение ст. 8 Конвенции по правам человека будет отсутствовать, если в деле превалируют вопросы публичных интересов общества, национальной безопасности государства и если вмешательство государства в частную жизнь соответствует основным положениям и. 2 ст. 8 Конвенции.

В деле *«Узун против Германии»*[51] заявитель был причастен к взрывам, совершенным левой экстремистской группировкой, что было подтверждено данными, полученными системой глобального позиционирования (*GPS*), которое было установлено в автомобиле по решению национальных властей. Полиции пришлось прибегнуть к использованию *GPS* после того, как заявитель вместе со своим предполагаемым сообщником уничтожил установленные ранее передатчики слежения в машине и практически перестал использовать мобильную связь, скрываясь от правосудия.

ЕСПЧ подтвердил, что подобное вмешательство соответствовало закону, преследовало законные цели предупреждения преступлений и защиты прав и свобод других лиц и было необходимо в демократическом обществе. Суд подчеркнул, что слежение за передвижением заявителя в общественных местах посредством GPS необходимо отличать от других методов визуального или акустического наблюдения, поскольку оно раскрывает меньше информации о поведении, мнении или чувствах человека и тем самым составляет меньшее вмешательство в его частную жизнь. В связи с этим ЕСПЧ не счел необходимым применять те же строгие гарантии против злоупотреблений, которые он разработал в своей прецедентной практике в отношении перехвата данных, полученных с помощью подобных систем.

Также ЕСПЧ признал, что единодушные выводы национальных судов о том, что наблюдение с помощью использования данных *GPS* было основано на национальном законодательстве, были разумно предвидимыми, поскольку соответствующие положения предусматривали использование технических средств, в частности, «для обнаружения местонахождения правонарушителя». Кроме того, в национальном законодательстве Германии установлены строгие стандарты авторизации бТО-наблюдения: оно может быть установлено только против лица, подозреваемого в совершении тяжкого уголовного преступления. В этом деле, по мнению ЕСПЧ, был соблюден и принцип пропорциональности: национальные власти начали использовать (хРб'-наблюдение только после того, как остальные методы оказались неэффективными, продолжительность наблюдения составило около трех месяцев, и было активным только в момент использования заявителем своей машины.

[51] *Uzun v. Germany*, постановление от 02.09.2010, жалоба № 35623/05.

Наблюдение за использованием Интернета, рабочих телефонов и электронной почты

Вопрос о правомерности наблюдения за использованием телефонов, электронной почты и Интернета рассматривался в деле *«Коплэнд против Соединенного Королевства»*[52]. Заявительница по данному делу занимала должность личного помощника директора в одном из учреждений высшего образования, которое одновременно являлось государственным органом (колледж, в котором работала заявительница, имел статус публичной организации, находящейся в государственном ведении). Как было установлено впоследствии, телефон заявительницы, ее электронная почта, а также вообще использование ею Интернета были подвергнуты наблюдению с целью установить, не осуществляет ли заявительница использование технического оборудования колледжа в личных целях. В частности, производился анализ телефонных счетов колледжа, которые содержали номера телефонов, по которым осуществлялись звонки, хранилась информация о датах телефонных звонков и их стоимости. В отношении использования Интернета с рабочего места производилось наблюдение за просмотренными страницами, а также времени, датах и продолжительности таких просмотров. Подобной проверке подверглась также личная корреспонденция заявительницы, о чем она не подозревала.

По смыслу ст. 8 Конвенции по правам человека государство несет на себе негативное обязательство воздерживаться от вмешательства в частную жизнь человека.

Государство-ответчик по этому делу придерживалось позиции, согласно которой получение таким образом информации, как и сама эта информация, не представляло собой вмешательство в частную жизнь и корреспонденцию заявительницы. Правительство указывало, что мониторинг сводился к анализу автоматически генерируемой информации, чтобы определить, использовались ли средства колледжа в личных целях; в отличие от упомянутого дела *«P.G. and J.H. против Соединенного Королевства»* фактического перехвата информации и дальнейшей ее переработки не происходило. Причем, по мнению государства-ответчика, в том случае, если подобные действия ЕСПЧ все же признает вторжением в частную жизнь, то такое вмешательство является оправданным по смыслу и. 2 ст. 8 Конвенции по правам человека.

ЕСПЧ пришел к выводу, что телефонные звонки, электронные сообщения и использование Интернета с рабочего места, по сути, включаются в категории «частная жизнь» и «корреспонденция». Заявительница не была предупреждена работодателем о том, что ее деятельность будет каким-либо образом отслеживаться. Она имела законные основания полагать, что использование рабочего оборудования в личных целях останется незамеченным. Таким образом, сбор и хранение информации, полученной исходя из такого вида наблюдения, были расценены Судом как вмешательство в частную жизнь и соответственно нарушающими ст. 8 Конвенции по правам человека.

К противоположному выводу ЕСПЧ пришел в ходе рассмотрения дела *«Барбулеску* против Румынии»[53]. Заявитель по настоящему делу был уволен работодателем после того, как было обнаружено, что он вел личную переписку в одном из мессенджеров с рабочего оборудования в течение рабочих часов. Работники этой компании уведомлялись о полном запрете использовать рабочее оборудование в личных целях – соответствующее положение содержалось в локальных актах компании.

ЕСПЧ подчеркнул, что помимо негативного обязательства воздерживаться от вмешательства в частную жизнь граждан, установленного ст. 8 Конвенции по правам человека, на государства – участников Конвенции возложены и позитивные обязательства, состоящие в

---

[52] *Copland v. the United Kingdom*, постановление от 03.04.2007, жалоба № 62617/00.

[53] *Bărbulescu v. Romania*, постановление от 12.01.2016, жалоба № 61496/08.

принятии определенных мер по защите права на неприкосновенность частной жизни. Граница между позитивными и негативными обязательствами государства не поддается точному определению. В обоих случаях следует учитывать баланс между конкурирующими интересами, который может включать личные и общественные интересы, которые расцениваются с точки зрения свободы усмотрения государства. Однако государства – участники Конвенции обязаны устанавливать достаточно четкие правила, регулирующие использование Интернета на рабочем месте.

В настоящем деле ЕСПЧ признал, что жалоба заявителя должна быть рассмотрена с точки зрения позитивных обязательств государства, поскольку он был нанят частной компанией, за действия которой не может быть ответственно государство. Исходя из этого ЕСПЧ не нашел в этом случае нарушений ст. 8 Конвенции.

С точки зрения позитивных обязательств государства следует обратить внимание на дело *«К. U. против Финляндии»*[54], в котором ЕСПЧ признал нарушение ст. 8 Конвенции по правам человека. Согласно обстоятельствам дела лицо, так и оставшееся неизвестным, поместило объявление сексуального характера на сайте знакомств от имени несовершеннолетнего лица (заявителя). Объявление содержало информацию о возрасте, годе рождения и физических характеристиках заявителя и указывало, что он искал интимных отношений с мужчиной. Оно также включало ссылку на страницу в Интернете, где можно было найти фотографию и номер телефона этого несовершеннолетнего. Соблюдая правила о конфиденциальности, хостинг-провайдер отказался раскрывать информацию о лице, разместившем объявление на сайте.

ЕСПЧ подчеркнул, что в данном случае имеет место нарушение неприкосновенности частной жизни несовершеннолетнего заявителя, которое могло привести к негативным последствиям в виде домогательств со стороны педофилов, создавало потенциальную угрозу его физическому и душевному благополучию. Суд отметил, что пользователи различных средств коммуникации и интернет-услуг должны иметь правовые гарантии неприкосновенности их частной жизни.

[54] *K.U. v. Finland*, постановление от 02.12.2008, жалоба № 2872/02.

Использование данных, полученных посредством фото- и видеосъемки

В практике ЕСПЧ встречаются дела, которые заканчиваются соглашениями о дружественном урегулировании, как это предусматривает ст. 39 Конвенции.

Например, в деле *«Фриедл против Австрии»*[55] заявитель был одним из организаторов демонстрации, направленной на привлечение внимания общественности к проблемам бездомных. Во время проведения демонстрации участники готовили еду, ели и спали на зонах для пешеходов, что стало причиной многочисленных жалоб от горожан. В соответствии с национальным законодательством Австрии любая демонстрация требует соответствующего разрешения, которое должны получить организаторы публичного мероприятия. Проводимая демонстрация требовала разрешения в соответствии с разд. 82 (1) Закона о дорожном движении, который категорически запрещает любые препятствия для пешеходных зон. Национальные власти настаивали на том, чтобы участники демонстрации покинули занимаемое место, что привело к противостоянию. В итоге полиция сделала фотографии демонстрантов для дальнейшего расследования инцидента. Заявитель, являющийся одним из участников демонстрации, счел, что его фотографии были сделаны полицией в индивидуальном порядке с целью идентификации его личности. С жалобой на нарушение права на защиту персональных данных заявитель обратился в Конституционный суд Австрии, но тот вынес решение, в котором признал, что не обладает достаточной юрисдикцией в вопросах использования персональных данных, полученных путем фотосъемки.

К моменту рассмотрения дела в ЕСПЧ в Австрии был принят Закон о службе безопасности, согласно которому независимые административные трибуналы приобрели юрисдикцию в вопросах, поднятых заявителем перед Конституционным судом Австрии. В связи с этим государство-ответчик подняло вопрос об исключении жалобы из списка рассматриваемых ЕСПЧ дел, на что не поступило возражений со стороны заявителя. Таким образом, исход дела был решен посредством дружественного урегулирования.

Однако в большинстве случаев государству-ответчику и заявителю не удается достигнуть дружественного урегулирования.

В деле *«Хмель против России»*[56] заявитель указывал, что осуществлением видеосъемки без его согласия в отделении милиции и последующей трансляции полученных данных по местному телевидению была нарушена ст. 8 Конвенции по правам человека. На тот момент заявитель являлся депутатом областной думы и был задержан при вождении автомобиля в нетрезвом состоянии. Приглашенные сотрудниками милиции журналисты произвели видеосъемку заявителя без его согласия и затем показали запись по телевидению. После этого частная жизнь заявителя стала объектом повышенного общественного внимания.

Государство-ответчик утверждало, что лицо, совершившее подобное правонарушение, должно претерпевать некоторые ограничения в отношении своих прав, включая право на уважение частной жизни.

По мнению ЕСПЧ, действия национальных властей нарушили ст. 8 Конвенции по правам человека. Суд отметил, что решение начальника милиции пригласить журналистов и разрешить им производить съемку без каких-либо ограничений на ее последующее использование, представляло собой вмешательство в право заявителя на неприкосновенность частной жизни, поскольку не соответствовало закону.

---

[55] *Friedl* v. *Austria,* решение об исключении жалобы из списка рассматриваемых дел от 31.01 Л995, жалоба № 15225/89.

[56] *Khmel* v. *Russia*, постановление от 12.12.2013, жалоба № 20383/04.

Дмитрий Дедов, судья ЕСПЧ от России, написал особое мнение по этому делу. Он указал, что ст. 3 Закона РФ от 18.04.1991 № 1026-1 «О милиции» устанавливала такие принципы уважения прав и свобод человека, как законность, гуманизм и гласность[57]. По его мнению, данное положение позволяет осуществлять вмешательство в право на неприкосновенность частной жизни, так как в данном случае милиция была обязана защитить свободу распространения информации.

Подводя итоги, можно признать, что соблюдение баланса между использованием преимуществ информационных технологий в публичных интересах и интересами личности имеет принципиальное значение при рассмотрении дела в Суде. Практика ЕСПЧ свидетельствует о том, что наиболее частые нарушения ст. 8 Конвенции по правам человека характерны для государств, где слабы процедурные гарантии или отсутствует надлежащее законодательство, позволяющее на национальном уровне обеспечить защиту права на неприкосновенность частной жизни в контексте использования информационных технологий. Отсутствие эффективных гарантий при сборе и хранении персональных данных, которые соответствовали бы требованиям п. 2 ст. 8 Конвенции по правам человека, остается проблемой для многих государств – участников Конвенции.

Важно заметить, что подход ЕСПЧ к разрешению дела в рассмотренной сфере зависит и от специфики сбора персональной информации. Это позволяет ЕСПЧ придерживаться закономерной позиции, согласно которой защита персональных данных имеет основополагающее значение для того, чтобы лицо пользовалось своим правом на неприкосновенность частной жизни в полном объеме.

[57] Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1991. № 16. Ст. 503.

Пристатейный библиографический список

1. *Samuel D. Warren, Louis D. Brandeis.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4, No. 5. P. 193.

2. *Глинская Н.П.* Юридический термин «privacy» как предмет системно-динамического исследования // Вестник Московского университета. Серия 19. Лингвистика и межкультурная коммуникация. 2010. № 2.

3. Российский ежегодник международного права. 1993—94. СПб., 1995. С. 340-376.

4. *Шугуров М.В.* Защита прав человека в условиях современного научно-технического прогресса: практика Европейского суда по правам человека // Международное публичное и частное право. 2011. № 1. С. 5.

Информационный брокер как новый субъект информационного права в эпоху Big Data (Москва, Россия)

Конец ознакомительного фрагмента.