УПРАВЛЕНИЕ

С.Н. МИХАЙЛУСОВ

АСПИРАНТ КАФЕДРЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ МЕЖДУНАРОДНОГО ИНСТИТУТА УПРАВЛЕНИЯ МОСКОВСКОГО ГОСУДАРСТВЕННОГО ИНСТИТУТА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ (УНИВЕРСИТЕТ) МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИИСКОЙ ФЕДЕРАЦИИ

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТА

В статье показывается, в какой мере те или иные области общественных отношений, возникающие в сети Интернет, урегулированы международным правом. Раскрывается роль «мягкого» права в международно-правовом регулировании Интернета.

Ключевые слова: международно-правовое регулирование, право интеллектуальной собственности, спам, киберпреступность, неприкосновенность частной жизни, электронная коммерция, содержание материалов Интернета, «мягкое» право, «жесткое» право.

S.MIKHAILUSOV

RESEARCH STUDENT, DEPARTMENT OF LEGAL SUPPORT FOR ADMINISTRATIVE WORK, INTERNATIONAL INSTITUTE OF ADMINISTRATION, MGIMO(UNIVERSITY) UNDER THE MINISTRY FOR FOREIGN AFFAIRS OF RUSSIA

INTERNATIONAL LEGAL REGULATION OF THE INTERNET

The article presents to what extent different spheres of social relations emerging in the Internet regulated by international law, reveals the role of the soft law concerning the international legal regulation of the Internet.

Key words: international legal regulation of the Internet, intellectual property rights, spam, cybercrime, privacy rights, e-commerce, Internet content, soft law, hard law.

Интернет – это глобальная виртуальная среда, происходящее в которой, несмотря на постоянные поиски технических решений, все еще сложно привязать к географическим границам. Природа Интернета позволяет работать в Сети максимально анонимно, дает возможность быть полностью мобильным и осуществлять деятельность из любой точки мира. Все это создает благоприятную среду для совершения противоправных действий. В таких условиях ни национальное законодательство, ни даже региональное не эффективны - успешно противодействовать злоупотреблению плодами ИКТ можно только на международном уровне.

Проследим, какие инициативы в области международно-правового регулирования Интернета уже нашли свое воплощение в форме правовых норм и какие вопросы еще предстоит решить.

В области защиты прав интеллектуальной собственности важной является деятельность Всемирной Организации Интеллектуальной Собственности (ВОИС). Договор ВОИС о защите авторских прав[1] и Договор ВОИС по исполнениям и фонограммам[2], принятые в 2002 году, обновили ранние инструменты (Бернская Конвенция об авторских правах, Парижская конвенция о патентах, торговых марках и зарегистрированных промышленных образцах, Римская конвенция) в свете появления новых цифровых технологий, в том числе Интернета. Так, ст. 4 Договора ВОИС о защите авторских прав устанавливает, что «компьютерные программы охраняются как литературные произведения в смысле Статьи 2 Бернской конвенции. Такая охрана распространяется на компьютерные программы независимо от способа или формы их выражения».

Другими крайне важными документами, разработанным ВОИС и принятым ICANN, стали Единая Политика Рассмотрения Споров о Доменных Именах[3] (UDRP) и Правила к Политике[4], призванные разрешать доменные споры между владельцами товарных знаков и администраторами доменов. На сегодняшний день UDRP принята всеми регистраторами в доменах .com, .net, .org, а также многими администраторами национальных доменов верхнего уровня[5].

Проблема борьбы со спамом в наибольшей степени демонстрирует необходимость международного подхода к ее решению. Так как спам может эффективно рассылаться из любой точки планеты, внутренние законы, запрещающие и

ограничивающие рассылку незапрашиваемой корреспонденции, практически не эффективны.

Против спама не существует международного инструмента; самым близким по значению можно назвать Директиву Европейского Союза «О неприкосновенности электронной частной жизни», требующую получение явного согласия адресата на получение рекламной и любой другой информации, в том числе по электронной почте[6].

Однако специалистами всего мира затрачиваются огромные усилия для противодействия рассылке незапрашиваемой корреспонденции. Например, в 2004 году был создан форум, известный как Лондонский план действий[7] (ЛПД). В форуме участвуют государственные и неправительственные организации из 27 стран, в число участников входят организации, ответственные за защиту персональных данных и прав потребителей, регулирование в области телекоммуникаций и представители коммерческого сектора.

Основываясь на последних достижениях таких организаций, как Организация экономического сотрудничества и развития (ОЭСР) и Специальная комиссия ОЭСР по спаму, Международный союз электросвязи (МСЭ), Международная ассоциация государственных органов, контролирующих соблюдение прав потребителей (ICPEN), Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС), а также на опыте ЕС, участники встречи приняли План действий. Его назначение – содействие международному сотрудничеству в области применения законодательства против спама и принятие мер в отношении сопутствующих спаму проблем таких, как он-лайн мошенничество, фишинг и распространение вирусов[8].

В 2006 году был создан Альянс по борьбе со спамом StopSpamAlliance[9]. Его цель - повышение эффективности координации международных действий в борьбе со спамом и, в конечном итоге, выработка соответствующего международного законодательства. В альянс входит большинство организаций, в той или иной степени занимающихся борьбой со спамом, в том числе и те, которые объединились в рамках ЛПД.

Касаемо киберпреступности также не существует полного международного инструмента, за исключением ни к чему не обязывающей резолюции Генеральной Ассамблеи ООН о Культуре мировой безопасности[10], которая основывается на более раннем документе, подготовленном ОЭСР[11]. Резолюция ООН лишь признает, что «действенная защита требует коммуникации и сотрудничества на национальном и международном уровнях между всеми заинтересованными сторонами и что национальные усилия должны подкрепляться эффективным, реальным международным и региональным сотрудничеством между заинтересованными сторонами».

Наиболее значимым документом является Конвенция Совета Европы по киберпреступности[12]. Под понятие киберпреступлений в конвенции подпадают правонарушения, совершенные в информационной среде, или против информационных ресурсов, или с помощью информационных средств. В примерный перечень этих деяний вошли: незаконный доступ в информационную среду, нелегальный перехват информационных ресурсов, вмешательство в компьютерную систему и информацию, содержащуюся на магнитных носителях, незаконное использование телекоммуникационного оборудования, подделка и мошенничество с применением компьютерных средств, а также преступления, относящиеся к детской порнографии и к нарушениям авторских и смежных прав.

В документе подробно описаны проблемы взаимодействия правоохранительных органов отдельных государств в ситуации, когда преступник и жертва находятся в разных странах и подчиняются разным законодательствам. Кроме того, конвенция оговаривает общие для всех интернет-провайдеров правила хранения личной информации клиентов на случай, если подобные сведения будут затребованы в ходе расследования киберпреступлений. Страны-участницы договора обязаны согласовать свое внутреннее законодательство с положениями конвенции, касающимися защиты частной жизни.

К этой конвенции так же присоединились такие неевропейские страны, как Южная Африка, Канада, США и Япония[13].

Международного стандарта неприкосновенности частной жизни в форме международного правового инструмента также не существует, хотя право на неприкосновенность частной жизни в общих понятиях признано в Статье 12 Всеобщей декларации прав человека[14] и Статье 17 Международного пакта о гражданских и политических правах. ООН также признала особую важность соблюдения неприкосновенности частной жизни лиц, чья личная информация хранится в электронных записях, посредством разработки рекомендаций к этой теме, которые были утверждены резолюцией Генеральной ассамблеи в 1990 году[15].

Существует ряд рекомендаций ОЭСР[16], принятых еще в 1980 году, приведших к созданию Концептуальной модели неприкосновенности частной жизни АТЭС, выпущенной ее Коор-

динационной группой по электронной коммерции (Electronic Commerce Steering Group)[17] в 2004, созданной с целью продвижения идеи о целостности информационной защиты частной жизни среди стран-членов АТЭС.

Другим региональным документом о неприкосновенности частной жизни, имеющим значительную важность в международном смысле является Директива ЕС о защите данных[18]. Одно из положений директивы гласит, что личные данные граждан ЕС не могут быть переданы «третьим странам» (т.е. странам, не входящим в ЕС), кроме стран обладающих собственными средствами защиты неприкосновенности частной жизни адекватного уровня[19].

В области регулирования электронной коммерции следует отметить деятельность Комиссии Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ). ЮНСИТРАЛ разработала два типовых закона – «Об электронной коммерции» и «Об электронных подписях»[20]. Оба закона принимались с учетом того, что в международной торговле все больше сделок заключается с помощью средств передачи данных, обычно именуемых электронной торговлей, и предусматривающих использование альтернативных бумажным формам методов передачи, хранения и подтверждения подлинности информации.

Кроме того, ЮНСИТРАЛ разработала конвенцию[21], цель которой прояснить такие правовые вопросы, как местоположение стороны контракта, созданного электронным образом, время и место исполнения контракта, использование автоматических систем обмена сообщениями при формировании контрактов, а так же формулировка критериев равенства между электронным и документарным обменом сообщений.

Последней рассматриваемой областью будет политика в отношении материалов в Интернете. Основные инициативы здесь опять-таки исходят от европейских стран, с их мощной правовой базой, касающейся проявлений различных форм нетерпимости, включая расизм и антисемитизм. Ключевым правовым инструментом, регулирующим вопросы содержания материалов Интернета, является Дополнительный протокол к Конвенции по киберпреступности Совета Европы[22]. Протокол описывает, какие виды нетерпимых высказываний должны быть запрещены в Интернете (расистские материалы, материалы, проповедующие геноцид, ксенофобию и преступления против человечности).

Значимой является деятельность Организации по безопасности и сотрудничеству в Европе (ОБСЕ). В 2003 году заседание ОБСЕ, посвященное свободе СМИ и Интернета, приняло так называемые Амстердамские рекомендации о свободе СМИ и Интернета[23]. Эти рекомендации направлены на защиту свободы слова и направлены на ограничение цензуры в Интернете.

Вместе с тем, в документе подчеркивается необходимость контролировать информацию, запрещенную международным правом.

Отметим, что свобода выражения убеждений и право искать, получать и распространять информацию - одно из основополагающих прав человека, которое обычно рассматривают в рамках обсуждения политики в отношении материалов Интернета и цензуры. В Декларации прав человека ООН свободе выражения убеждений противопоставляется право государства ограничивать такую свободу в интересах удовлетворения справедливых требований морали, общественного порядка и общего благосостояния (ст. 29). Таким образом, и обсуждение, и претворение в жизнь ст. 19 должны рассматриваться в контексте достижения должного баланса между двумя этими потребностями.

Таким образом, хотя в области международно-правового регулирования Интернетом используется широкий набор инструментов (конвенции, договоры, декларации, рекомендации и пр), не все грани общественных отношений в Сети имеют на сегодняшний день четкую правовую основу. Причины, как думается, кроются в политической, культурной, правовой и идеологической неоднородности мира, затрудняющей выработку международных правовых норм.

Так, внутренние подходы к вопросу о содержании глобальной сети варьируются от максимального невмешательства со стороны государства (США), до крайне строгой цензуры (Куба, Китай, Вьетнам и др.) Посередине находятся такие страны, как Франция, Великобритания, Канада, Австралия и др., где запрещены некоторые типы он-лайн контента.

Другая проблема видится в динамизме развития информационных и коммуникационных технологий. Процесс формирования правовых механизмов, в основе которых лежит международное право, громоздок, трудоемок, требует значительных финансовых затрат, в результате чего сильно отстает от темпов внедрения новых ИКТ. Не удивительно поэтому, что в контексте управления Интернетом особенно актуальным становится деление международного права «жесткое», определенное Статутом Международного суда[24], и так называемое «мягкое», не создающие правовых обязательств.

Разница между «мягким» и «жестким» правом – это разница между руководящими принципами и имеющими обязательную силу правилами. «Жесткое» право реализуется по принципу

«кнута и пряника», «мягкое» - через обмен информацией, что в итоге способствует выработке консенсуса[25]. Последний процесс менее затратный как с финансовой, так и с точки зрения затраченных усилий и времени, но, между тем, предполагает участие гораздо большего числа заинтересованных сторон.

Велижанина М.Ю. дает следующее определение «мягкому» праву – «это совокупность юридически необязательных международных норм, создаваемых государствами, международными организациями, не противоречащих основным принципам и нормам международного права и направленных на регулирование международных отношений. Эти нормы не содержат международно-правовых обязательств и закрепляются в рекомендательных актах международных организаций, многосторонних, двусторонних и односторонних политических актов государств»[26].

Учитывая, что многие страны имеют собственное видение политики в отношении управления Интернетом, «мягкое» право становится незаменимым механизмом международно-правового регулирования глобальной сети.

[1] WIPO Copyright Treaty, http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html

[2] WIPO Performances and Phonograms Treaty (WPPT), http://www.wipo.int/treaties/en/ip/wp pt/trtdocs_wo034.html

[3] Uniform Domain Name Dispute Resolution Policy, http://www.icann.org/en/udrp/udrp-policy -24oct99.htm

[4] Rules for UDRP, http://www.icann.org/en/udrp/udrp-rules-24oct99.htm

[5] Серго А.Г. Доменные имена. С. 108.

[6] Directive 2002/58/EC of 12 July 2002 On Privacy and Electronic Communications, para 40, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

[7] London Action Plan.

[8] Подробнее см.: http://www.londonactionplan.org/?q=node/29

[9] http://stopspamalliance.org

[10] General Assembly of the United Nations, Creation of a Global Culture of Cybersecurity: Resolution , 2003, http://daccessdds.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf ?OpenElement

[11] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002, обзор документа см.: http://www.oecd.org/dataoecd/16/0/15582276.pdf

[12] Convention on Cybercrime, 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[13] См.: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=6/5 /2009&CL=ENG

[14] http://www.un.org/russian/documen/declarat/declhr.htm

[15] Revised version of the Guidelines for the Regulation of Computerized Personal Data Files prepared by Mr. Louis Joinet. http://daccessdds.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G90 10708.pdf?OpenElement

[16] http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[17] См.: http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html

[18] EC Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, http://ec.europa.eu/justice_home/fsj/privacy/law/ index_en.htm

[19] Para 56, 57.

[20] ЮНСИТРАЛ, Типовой закон об электронной коммерции, 1996 г., http://www.un.org/russian/documen/convents/commerce.pdf; Типовой закон об электронных подписях, 2001 г., http://www.un.org/russian/documen/convents/uncitral.pdf

[21] UN Convention on the Use of Electronic Communications in International Contracts, 2005, http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

[22] CE Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003, http://conventions.coe.int/Treaty/EN/Treaties/HTML/189.htm

[23] Amsterdam Recommendations, Freedom of the Media and the Internet, 2003, http://www.osce.org/documents/rfm/2003 06215_en.pdf

[24] Статут Международного суда. ст. 38. п. 1.

[25] Anne-Marie Slaughter. Governing the Global Economy through Government Networks, The Role of Law in International Politics: Essays in International Relations and International Law, Oxford University Press, 2000.

[26] Велижанина М. Ю. «Мягкое право»: его сущность и роль в регулировании международных отношений : дисс. ... кан. юр. наук. М., 2007. С. 31.