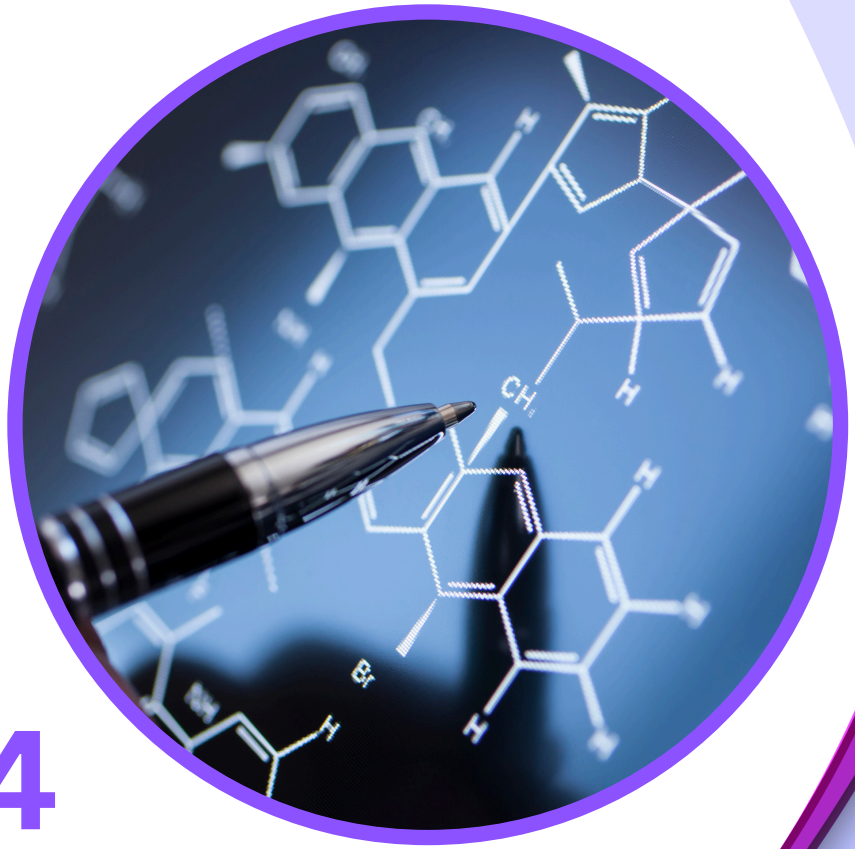
Science Conference

www.science-conference.com

a digital platform dedicated to disseminating a wide array of scientific research articles and papers. It serves as a valuable resource for the scientific community and others interested in cutting-edge scientific knowledge and insights.



2024

№ 1 (2)

TABLE OF CONTENTS

ЗАЩИТА ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА В КИБЕРПРОСТРАНСТВЕ

Салауат Конысбаев

Студент магистратуры Ташкентского
государственного юридического университета

salauat.konisbaev@gmail.com

АННОТАЦИЯ

В данной статье рассматривается необходимость и сложности международного регулирования киберпространства. Подчеркивается важность заключения международного соглашения, которое будет обеспечивать правовую основу для определения юрисдикции в киберпространстве. Автор указывает, что индивидуальные усилия отдельных государств недостаточны для эффективного регулирования этой сферы, и что необходимо сотрудничество на уровне международного права, в первую очередь под эгидой Организации Объединенных Наций (ООН).

КЛЮЧЕВЫЕ СЛОВА

Государственное регулирование, киберпространство, юрисдикция, международное право, информационные и коммуникационные технологии, международная безопасность, суверенитет.

Поскольку наши общества становятся все более зависимыми от информационных и коммуникационных технологий, обеспечение международного соглашения по регулированию киберпространства, определение юрисдикции, стало одним из наиболее важных вопросов нашего времени.

В рамках международного публичного права юрисдикция означает «сферу суверенной власти государства по законодательству, суду, управлению» в то время как в области международного частного права термин «юрисдикция» употребляется в смысле международной подсудности, т.е. компетенции судебного аппарата данного государства по разрешению определенного рода гражданских дел. При этом второе значение вытекает из первого: способность судебных органов рассматривать споры является следствием права суверенной власти государства[1].

Для государственного регулирования юрисдикции в киберпространстве надо принять международный договор, унифицированную норму, по которому все страны должны быть заинтересованы в её ратификации, а для осуществления этой цели требуется взаимодействие, сотрудничество стран. Самой влиятельной организацией в рамках принятия конвенции, участниками которой являются почти все страны мира - это Организация Объединненых Наций.

Отдельная, суверенная страна не может единолично принимать законы по урегулированию, применению своей юрисдикции в отношении киберпространства, так как в нём взаимодействуют все граждане, субъекты государств. В связи с этим надо обращаться к международному публичному праву для нахождения консенсуса.

Андерс Хенриксен, в своей статье отмечает, что с тех пор как проблемы ИКТ были впервые доведены до сведения Генеральной Ассамблеи ООН в конце 1990-х годов, так называемый «процесс ООН ГПЭ» стал основным направлением межгосударственного диалога о международно-правовом регулировании киберпространства[2].

Группы правительственных экспертов (далее именуется как «ГПЭ»), созданные Генеральным секретарем ООН, обсуждали, как решать

проблемы, связанные с новыми технологиями. Несмотря на начальные трудности, впоследствии было достигнуто несколько важных соглашений, включая признание того, что киберпространство регулируется международными правовыми принципами.

Однако в июне 2017 года пятая группа правительственных экспертов не смогла договориться о новом отчете, что привело к тупику. Это было предсказуемо, поскольку регулирование ИКТ затрагивает не только право, но и стратегию, политику и идеологические разногласия. Различия в интересах и нормативных предпочтениях государств оказались слишком велики для достижения консенсуса.

В 1998 году Россия представила проект резолюции в Первом комитете Генеральной Ассамблеи ООН, обращая внимание на угрозы, связанные с новыми информационными и коммуникационными технологиями (далее именуется как «ИКТ»). В последующие годы Россия продолжала вносить аналогичные проекты резолюций, что в 2002 году привело к созданию первой группы правительственных экспертов (ГПЭ) для изучения вопросов безопасности ИКТ.

Первая ГПЭ, состоящая из 15 членов, не смогла прийти к консенсусу по итоговому отчету. Однако ООН продолжила свои усилия, и в 2005 году была создана вторая группа экспертов, которая в 2010 году опубликовала краткий отчет с основными выводами и рекомендациями. Этот отчет, хоть и не внес значительной юридической ясности, стал важным шагом вперед, так как свидетельствовал о возможности достижения согласия.

Третья ГПЭ, созданная в 2011 году, в 2013 году представила отчет, подчеркивающий, что международное право, включая Устав ООН, применяется к киберпространству. Этот отчет также признал, что права человека и основные свободы действуют в ИКТ, и что государства должны соблюдать принципы суверенитета и невмешательства.

В 2013 году была сформирована четвертая ГПЭ, которая в 2015 году представила отчет с более детальными рекомендациями о применении международного права в ИКТ. Отчет подтвердил, что государства должны соблюдать свои международные обязательства, и что существующие

принципы международного права применимы к кибердеятельности. Однако в нем не было четко указано, что международное гуманитарное право применимо к кибероперациям.

В 2017 году пятая группа экспертов не смогла договориться о новом отчете, что привело к тупику в процессе ГПЭ. Основные причины провала заключались в стратегических, политических и идеологических разногласиях между государствами, которые сделали невозможным достижение консенсуса по ряду важных вопросов.

К примеру, Китай стремится предотвратить применение международного гуманитарного права к кибердеятельности, поддерживая ограничительную позицию в отношении законности применения силы. Китай хотел бы, чтобы ООН взяла на себя ведущую роль в регулировании ИКТ, критикуя процесс Таллиннского руководства как попытку США и НАТО сохранить свое доминирование. Россия также использует международное право для противодействия американскому влиянию и стремится к международному соглашению по образцу соглашений о контроле над вооружениями. Россия считает, что такие соглашения помогут уравнять правила игры.

В свою очередь США стремятся сохранить свое доминирующее положение в киберпространстве, используя международное право для предотвращения участия других государств в подрывной деятельности. США противостоят новым правовым ограничениям, которые могли бы ограничить их кибервозможности, и предпочитают регулировать киберпространство существующими правовыми принципами. США активно борются с промышленным шпионажем и кражей интеллектуальной собственности, убеждая Китай принять норму, запрещающую экономический шпионаж, и преследуют китайских граждан за кибершпионаж.

Что касается остальных государств, то некоторые государства предпочитают не участвовать активно в создании детального регулирования ИКТ, ожидая, куда движется технология, или сохраняя существующую правовую неопределенность для большей гибкости. Это

может быть стратегическим ходом для сохранения свободы действий в киберпространстве.

Фундаментальные идеологические разногласия по поводу открытости Интернета и основных свобод затрудняют достижение общей позиции по регулированию ИКТ. Одни государства рассматривают свободный поток информации как благо, другие — как угрозу. Западные государства считают киберпространство важным для прав человека, таких как свобода выражения, и обсуждают «кибербезопасность» с акцентом на мирное использование. В России, Китае и на Ближнем Востоке открытое киберпространство воспринимается как угроза государственному суверенитету, и обсуждения сосредоточены на «информационной безопасности».

На Всемирной конференции по международной электросвязи (англ. WCIT) 2012 года многие западные государства отказались подписать поправки к Регламенту международной электросвязи, опасаясь усиления государственного контроля над киберпространством. В 2011 году Шанхайская организация сотрудничества (ШОС), включающая Китай, Россию и другие страны, представила Международный кодекс поведения по информационной безопасности, подчеркивающий необходимость защиты государственного суверенитета и введения ограничений на информацию для защиты национальной безопасности.

По мнению Андерса Хенриксена, в своей статье отмечает, что трудности, с которыми сталкиваются государства в достижении соглашения по регулированию ИКТ, не являются чем-то новым. Исторически, государствам всегда требовалось значительное время для согласования подходов к новым технологиям и их регулирования[3].

В целом можно согласиться с Хенриксеном, так как договориться в применении юрисдикции в кибепространстве требует значительного времени, в связи с разными интересами суверенных государств.

Аналогию можно провести с международным торговым правом, где глобальные соглашения застопорились, и государства ищут региональных

партнеров. Так же, как в торговле, в регулировании ИКТ акцент смещается на региональные и двусторонние инициативы.

После провала пятой группы экспертов ООН в 2017 году, США заявили о намерении работать с меньшими группами партнеров-единомышленников и следовать двусторонним соглашениям. Китай и Россия создали Шанхайскую организацию сотрудничества, которая предложила ООН Кодекс поведения по информационной безопасности. В Европе Совет Европы принял Конвенцию о киберпреступности, а ОБСЕ установила меры доверия для повышения киберстабильности.

Автор данной статьи считает, что региональные соглашения могут ускорить принятие норм, избегая длительных переговоров. Однако, это может привести к фрагментации международного права, создавая «бункеры» норм в разных регионах.

В заключении стоит отметить, что несмотря на тупиковую ситуацию в ООН, усилия по внесению правовой ясности в регулирование киберпространства продолжатся, но чтобы государств пришли к консенсусу требуется время.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

[1] Мажорина М.В. Киберпространство и методология международного частного права // Право. Журнал Высшей школы экономики. 2020. №2. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-i-metodologiya-mezhdunarodnogo-chastnogo-prava (дата обращения: 04.06.2024).

[2] Андерс Хенриксен, Конец пути процесса ГПЭ ООН: Будущее регулирование киберпространства, Журнал кибербезопасности , Том 5, Выпуск 1, 2019 г. // URL: https://doi.org/10.1093/cybsec/tyy009.

[3]Андерс Хенриксен, Конец пути процесса ГПЭ ООН: Будущее регулирование киберпространства, Журнал кибербезопасности , Том 5, Выпуск 1, 2019 г. // URL: https://doi.org/10.1093/cybsec/tyy009.