Секция «Международное частное право»

**Суверенитет государства в киберпространстве**

***Озманян Юсуб Зограбович***
*Студент (бакалавр)*
Новосибирский национальный исследовательский государственный университет,
Новосибирск, Россия
*E-mail: ozmanyan.y@mail.ru*

Интернет трансграничен, его инфраструктура позволяет пользователю иметь доступ к информации в любой точке мира, достаточно лишь минимального технического обеспечения. Цифровизация ставит новые вызовы перед правом, в том числе международным. Новые возможности порождают и новые проблемы: хакерские атаки, трансграничная цифровая преступность, вмешательство в государственную киберинфраструктуру.

Киберпространство - это взаимосвязанные сети, системы и устройства, при помощи которых пользователи имеют возможность создавать, использовать, хранить, модифицировать, и обмениваться информацией [4]. Киберпространство нельзя измерить как физическое пространство по таким критериям, как место, дистанция, размер и направление [1]. Киберпространство разделяют на уровни в котором технологическое оборудование (сервера, сети) образует физический уровень киберпространства. Он — это основа киберпространства, но без иных уровней («информационного» и «человеческого») киберпространство бессмысленно [2].

В рамках Вестфальской модели суверены признают друг за другом власть в пределах своих владений, то есть физического пространства, ограниченного географическими границами [6]. По мнению некоторых исследователей, безграничный и атерриториальный характер киберпространства делает его несовместимым со стандартной системой международно-правового регулирования, основанной на совпадении физического пространства, представляемого государствам, и их «правового пространства» [3]. Другие специалисты отмечают, что киберпространство не обладает иммунитетом от государственных суверенитетов, поскольку оно состоит из людей и инфраструктуры, которые существуют физически, а значит неотделимы от государственных границ [5]. Так, официальная позиция МИД ФРГ также заключается в том, что нет никаких «киберграниц» в киберпространстве, отдельных от государственных границ в физическом плане [7].

Последний подход представляется более обоснованным. Во-первых, установление для киберпространства режима «всеобщего достояния» затруднительно — значительная часть серверов и сетей находятся в частной собственности, а некоторая в государственной. Во-вторых, установление наднационального регулирования киберпространства поставит под сомнение сам факт распространения суверенитета на граждан государства, которые являются создателями, хранителями и потребителями контента.

Действие суверенитета часто рассматривается в зарубежной доктрине в контексте концепции юрисдикций.

Преобладание территориального принципа юрисдикции для актов, совершенных в киберпространстве, неизбежно будет порождать конфликты юрисдикций. Такие конфликты возникают, когда деяние совершено в одной стране, а его последствия проявляются в другой, или даже нескольких странах. Показательно дело «LICRA v Yahoo!», рассмотренное Трибуналом большой инстанции Парижа. Суд признал, что продажа интернет-аукционом «Yahoo!» нацистской атрибутики является преступлением, совершенным на территории Франции, несмотря на то, что деятельность сервис «Yahoo!» осуществлял в США, поскольку доступ к сайту имели французские пользователи, а «Yahoo!» имел намерение

продавать на территории Франции, демонстрируя рекламу на французском языке. Трибунал предписал компании принять меры к предотвращению доступа к нацистским товарам под угрозой существенного штрафа [8]. Ситуации конфликта юрисдикций могут быть разрешены с учетом опыта американского права и их инструментария: «статута длинной руки» основанного на принципах минимальной связи.

В контексте киберпространства такая минимальная связь может выражаться в том, что деятельность ответчика имеет направленность на пользователей из конкретного государства. Такая направленность имеет место, когда какой-либо акт совершен ответчиком на сайте в национальной доменной зоне, поскольку большинство пользователей, например, российского сегмента интернета - россияне. Направленность на пользователей имеется и в том случае, если для совершения нарушения использовался сайт, имеющий раздел на одном из национальных языков.

Предполагается, что непосредственное кибервмешательство в цифровую инфраструктуру государства является контактом значительнее минимального, а потому юрисдикция пострадавшей страны основывается на принципе пассивной национальности и защитном принципе.

Таким образом, существующий инструментарий международного права достаточен для разрешения вопросов, связанных с юрисдикцией в киберпространстве. Полагается, что существующие механизмы достаточно адаптивны и будут развиваться вместе с техническим прогрессом.

**Источники и литература**

1) Bryant R. What Kind of Space is Cyberspace? // Minerva - An Internet Journal of Philosophy. 2001. №5. Pp. 138–155.

2) Clark D. Characterizing Cyberspace: Past, Present, and Future // ECIR Work. Pap., vol. 2010, no. Version 1.2, pp. 1–18, 2010.

3) Johnson D.R., Post D.G. Law and Borders: The Rise of Law in Cyberspace// Stanford Law Review No 11(5) (2006)

4) Kuehl D.T. 'From cyberspace to cyberpower: Defining the problem' in Franklin D Kramer, Stuart H Starr and Larry K Wentz, Cyberpower and National Security // National Defense University Press 2009. No 28.

5) Liaropoulos A. Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? // Journal of Information Warfare. Vol. 12, No. 2 (2013), pp. 19-26

6) Scassa, T. Currie. R. J. New First Principles: Assessing the Internet's Challenges to Jurisdiction. // Georgetown Journal of International Law 42 (4). 2010. 1018 pp.

7) On the Application of International Law in Cyberspace Position Paper // Website of Foreign Office of FRG. March 2021 URL: https://clck.ru/bnHoA (дата обращения: 22.02.2022).

8) Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme. 145 F. Supp. 2d 1168 (N.D. Cal. 2001)//URL: http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/YahooVLicra.pdf (дата обращения: 22.02.2022).