Фарзуллаева А.Э. ♦

DOI: 10.25108/2304-1730-1749.iolr.2021.65.73-79
УДК: 342.4

Угрозы цифровому суверенитету государства

Аннотация: Рассматриваются возможные угрозы цифровому суверенитету государства. Проведенный анализ позволяет в процессе дальнейшего исследования рассматривать информационный суверенитет как способность технологически и законодательно обеспечивать и защищать независимость государства и конституционные права граждан в информационном пространстве от внешних угроз. Информационный суверенитет включает возможности государства соответствии с Конституцией и всей национально-правовой системой, а так же международным правом самостоятельно и независимо, с соблюдением баланса интересов личности, общества и государства, определять и защищать национальные интересы в информационном пространстве и обеспечивать информационную безопасность государства.

Ключевые слова: информация; угроза; государство; цифровой суверенитет.

Современный период мирового развития характеризуется высокой динамикой усиления влияния информационной сферы как стратегического государственного ресурса, включающего административно-юрисдикционную и технократическую составляющие государственного цифрового суверенитета. Западная правовая доктрина толкует понятие суверенитет в двух направлениях: по субъекту - государственный, народный, национальный и по объекту – экономика, оборона, культура и т.д. В силу масштаба и значимости информационной сферы в глобализационном развитии особую актуальность приобретают вопросы конституционно-правовой защиты информационного суверенитета государства. Пути достижения соразмерности и соблюдения баланса интересов личности, общества и государства на основе конституционного права при обеспечении информационной безопасности анализируются в актуальном для конституционно-правовой науки дискурсе формирования публично-правовой доктрины информационного суверенитета как государственного суверенитета в информационном пространстве. Развитие сети интернет, являясь следствием пятой информационной революцией, стало актуальным вызовом конституционно-правовому обеспечению информационного суверенитета всех государств.

В настоящее время традиционное понятие территориального суверенитета дополняется понятием цифровой суверенитет вследствие развивающихся в виртуальном пространстве информационных и экономических отношений, приобретающих свойства экстерриториальности.

Государственный суверенитет применительно к информационной сфере выступает декларируемым конституцией правом государства независимо от внешнего влияния самостоятельно определять развитие общественных отношений по поводу информации и информационной инфраструктуры как объектов интересов личности, общества и государства. Технологически в конце XX века национальная информационная среда достаточно быстро и открыто трансфор-

♦ **Фарзуллаева Афет Эльхан кызы** – диссертант Института права и прав человека НАНА (Азербайджан). E-mail: afatgahramanova@gmail.com

мировалась в глобальную информационную инфраструктуру, современное развитие которой на экстерриториальной основе идет ускоренными темпами.

Можно констатировать, что формирующаяся в науке конституционного права концепция информационного суверенитета расширяет географический традиционно-территориальный признак, дополняя его признаком киберпространства как экстерриториальной структурой виртуального пространства, не отражающего географически-государственного деление мирового пространства. Цифровой суверенитет распространяется на информационное пространство как «виртуальную территорию, принадлежащую государству, наполненную информацией, технологическими ресурсами ее сбора, обработки, хранения, распространения и пользователями информационных ресурсов, подпадающими под юрисдикцию законодательства, действующего на этой территории» [2]. Суверенные права государства в наднациональном пространстве постоянно подвергаются рискам и угрозам, так как в непрерывном временном режиме происходит электронный обмен данными, который не зависит от географического местонахождения субъектов.

Субъекты интернет-отношений наднационального пространства должны отвечать требованиям международного и национального законодательства в части право-, дее- и деликтоспособности. В 2015 г. на 70-й сессии Генеральной Ассамблеи ООН Группа правительственных экспертов ООН по международной информационной безопасности подтвердила суверенное право государств распоряжаться информационно-коммуникационной инфраструктурой на своей территории и определять свою политику в сфере международной информационной безопасности [3]. Всеобъемлющая международно-правовая база, регламентирующая защиту цифрового суверенитета государства, до настоящего времени не создана, равно как не унифицированы международные подходы к самой проблеме защиты цифрового суверенитета. Международные усилия сосредотачиваются в основном на узкой области вопросов, в частности, касающихся конфиденциальности данных.

В. Гонг понятие государственный информационный суверенитет предлагает анализировать через конституционно закрепленные внутреннюю и внешнюю функции государства. Внутренний информационный суверенитет, определяемый В. Гонгом как «жесткий», означает право высшей власти на реализацию информационной политики, обеспечение информационной безопасности, фактический контроль над потоком политической, культурной, социальной и другой информации, циркулирующей в виртуальном пространстве в целом. Внешний суверенитет, определяемый как «мягкий», «проявляется в полном юридическом равенстве государств и их независимости от внутреннего контроля при производстве и использовании информации» [2, с. 120-124].

Среди правоведов СНГ конституционно-правовое регулирование информационного суверенитета государства рассматривается в основном не как направление информационной безопасности, а в парадигме реализации информационной политике в информационном обществе. В частности, Д. Абдрахманов считает, что обеспечение государственного суверенитета в информационной сфере приводит к сдерживанию процессов, направленных на развитие информационного общества. М. Кучерявый предлагает определять информационный суверенитет как «верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве» [4, с. 11].

Современные информационные ресурсы и их инфраструктура отличаются от других объектов, регулируемых правом, уникальными свойствами делимости и воспроизводимости, а их пространственные характеристики выходят за пределы государственной территории. Внешние и внутренние угрозы информационному суверенитету государства имеют долгосрочный и многопрофильный характер, что оказывает существенное влияние на формирование и реализацию как стратегии, так и тактики защиты цифрового суверенитета государства. При всех позитивных аспектах развития цифровых технологий они уже становятся инструментом межгосударственного противоборства, криминальной и террористической деятельности международном масштабе.

Американский исследователь Т. Джонсон приводит статический анализ, свидетельствующий о возрастающей динамике совершаемого в интернет-пространстве мошенничества, распространения порнографических, пронаркотических и экстремистских материалов, клеветы, оскорблений и других подобных нарушений, угрожающей в совокупности безопасности цифрового суверенитета государства. Угрозы, исходящие от информационно-коммуникативных технологий, определяются их широкими возможностями воздействовать на конституционные основы государства. В частности, латентно влиять на политические решения и социально-политическую стабильность в государстве; пропагандировать насилие, ксенофобию, разжигать межнациональные и межконфессиональные конфликты. Особую угрозу цифровому суверенитету государства представляет создание деструктивных экстерриториальных сетевых сообществ, пропагандирующих терроризм, экстремизм, сепаратизм и вербующих участников незаконных вооруженных формирований. Развитие интернет-технологий расширяло пространство источников и форм угроз информационному суверенитету, обусловленные противоправным использованием информационных и коммуникационных технологий. Эти угрозы связаны с увеличением числа преступлений, связанных с нарушением конституционных прав и свобод человека, неприкосновенности частной жизни, защиты персональных данных, роста масштабов компьютерной преступности в кредитно-финансовой сфере. Совокупность элементов воздействия угрозы включает источники, обстоятельства, предпосылки, мотивы объекты, виды и способы негативного воздействия. Спецификой угроз цифровому суверенитет государства составляет фрагментация составов преступлений и методов борьбы с ними по отдельным государственным юрисдикциям, а также трудность в определении физического местонахождения «ведут к появлению «безопасных гаваней» для субъектов информационных отношений, пользующихся несовершенством международно-правовой базы и правоприменительной практики отдельных государствах» [1].

Информационный ресурс, выступающий индикатором успешного технологического развития страны, может носить характер как информационно-технического, так и информационно-психологического оружия, направленного против государственного информационного пространства другого государства и нанесения противоборствующей стороне максимального урона. Внедрение информационных технологий наращивает возможности информационно-технического воздействия на информационную инфраструктуру в военных целях, что существенно повышает вероятность информационных угроз государственному суверенитету. Через вирусные программы, программы-роботов, т.е. программные средства, взламывающие критически важные объекты информационно-коммуникационной инфраструктуры можно воздействовать на важные объекты государственного и военного управления, производственную и экономическую сферу, вызывать необратимые негативные изменения в функционировании объектов инфраструктуры суверенных государств.

Интенсивное развития атакующих виртуальных технологий по сравнению с защитными технологиями даже у стран – лидеров высоких технологий свидетельствует о том факте, что полнотой и суверенитета не обладает ни одно государство, но уровень его суверенности в информационной безопасности в разных странах различный. Интенсивно развивается информационное оружие с целью вторжения в цифровое пространство других государств. Европейские правоведы Р. Полсак и Д. Свантессон высказывают мысль, что само содержание понятия государственного суверенитета в связи с развитием информационно-коммуникативных технологий требует разработки нового нормативного содержания, так как такой атрибут государственного суверенитета как государственные границы теряет смысл.

На начальном этапе информационной глобализации регулирование информационной сферы в значительной мере основывалось не на международных договорах, а на документах международных организаций, каждая из которых по своему трактовала угрозы информационной безопасности государства. В настоящее время угрозы цифровому суверенитету государству усиливают тенденцию суверенизации в правовом регулировании информационных отношений. Аналитик Стэндфордского университета Е. Морос пишет, что возврат к национально-правовому внутригосударственному регулированию проявляется в сфере конституционно-правового регулирования информационных отношений, в создании правовых основ для отказов от исполнения, в частности, решений международных судов.

Эксперт ООН по правовым аспектам информационного общества Т.Фуентес-Камачо доказывает, что не только развитие технологий угрожает информационному суверенитету, но и сетевая субъектная среда современного информационного пространства, то есть «граждане разных стран, возрастов и профессий поставляющие и принимающие информацию через всемирную сеть компьютеров, взаимосвязанных средствами коммуникационных инфраструктур, обеспечивающих цифровую обработку и передачу информации» [7, с. 511]. Действия субъектов интернет-среды в определенных случаях могут совершаться с целью подрыва конституционного строя как основного признака государственного суверенитета.

Проблема сетевого саморегулирования создает самые значительные угрозы информационному суверенитету, так как сетевая саморегуляция присуще транснациональным субъектам наркопроизводства и порнопроизводства, банковским системам, которые связаны с «отмыванием» денег, сепаратистским, экстремистским и террористическим структурам. По данным исследования «Как современный терроризм использует интернет» тенденция виртуального присутствия террористических групп характерна для всех регионов мирового пространства, однако 90% всей террористической активности, включая пропаганду радикализма и экстремизма, ведется в Интернете с использованием социальных сетей. Сама сетевая конструкция, не управляемая из какого-то определенного центра, с высокой скоростью передачи информации и со свободным к ней доступом, программируется с возможностью блокировки контролирующих функций государства.

В западноевропейской правовой науке постулируется концепция снижения роли конституционно-правового регулирования информационного суверенитета государства. Ряд международных экспертов в области правового регулирования информационной безопасности считает, что традиционное понимание государственного суверенитета как верховенства государственной власти внутри страны и ее независимости в международных отношениях может быть применено с целым рядом оговорок. Государства, признавшие конституционно-правовыми нормами свой национальный суверенитет в обеспечении безопасности критиче-

ской информационной инфраструктуры, будут способствовать снижению информационной активности в целом всей страны и пользователей, в частности.

В западноевропейской правовой науке постулируется концепция снижения роли конституционно-правового регулирования информационного суверенитета государства. Американский правовед Б. Карпентер считает, что интернет следует рассматривать как terranullius, то есть территорию, не находящуюся под суверенитетом какого-либо государства. Правовой государственный контроль существующих, как государственных, так и частных систем информационной безопасности, ведет к снижению страновой виртуальной активности и следующей за ней сужения виртуального пространства. Нам представляется такая позиция весьма спорной, так как разработка и создание механизмов формирования и реализации информационной безопасности представляет главную функцию государства в этой сфере. Мы поддерживаем обоснованную профессором права Лейденского университета Г. Крейженом концепцию информационного суверенитета как права правительства контролировать информационные потоки в рамках своих территории.

В целом в зарубежной правовой науке с учетом объективно сложившейся в трансграничном пространстве многоуровневой глобальной технологической инфраструктуры интернета и специфики функционирования ее базовых компонентов сформировался подход определять угрозы цифровому суверенитету государства общего характера и угрозы отдельным элементам цифрового суверенитета государства. Основными угрозами общего характера информационному суверенитету государства являются следующие: а) использование информационных и коммуникационных технологий как информационного оружия в военно-политических целях для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государства; б) использование ИКТ в экстремистских и террористических целях для пропаганды воинственного радикализма, для вербовки новых сторонников, финансирования, обучения, подстрекательства и проведения терактов; в) деструктивное воздействие на системы управления важными социальными и промышленными объектами, экономическая информационная война, информационный терроризм как проведение хакерских атак на элементы критической информационной инфраструктуры; г) деструктивное использование ИКТ для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию; д) угрозами отдельным элементам цифрового суверенитета государства выступают: е) физическая инфраструктурная составляющая, в частности, оптические кабельные сети, находящиеся на территории одного государства, которыми относительно свободно могут использоваться практически любым субъектом, как государственным, так и негосударственным, в том числе и против интересов этого государства; ж) защита от несанкционированного доступа к персональным данным граждан, если данные циркулируют в сетях открытого или полуоткрытого типа, поскольку, как показали разоблачения Э. Сноудена, некоторые страны занимаются массированным съёмом информации на самих каналах связи; з) защита данных, обрабатываемых вне юрисдикций национального законодательства, если все технические мощности серверов находятся за пределами юрисдикции государства; к) уязвимость перед технологическими санкциями, введение ограничений на поставки оборудования, изменение бизнес интересов поставщиков технологий и оборудования.

Проведенный выше анализ позволяет нам в процессе дальнейшего исследования рассматривать информационный суверенитет как способность технологически и законодательно обеспечивать и защищать независимость государства и конституционные права граждан в информационном пространстве от внешних угроз. Информационный суверенитет включает возможности государства соответствии с Конституцией и всей национально-правовой системой, а так же международным правом самостоятельно и независимо, с соблюдением баланса интересов личности, общества и государства, определять и защищать национальные интересы в информационном пространстве и обеспечивать информационную безопасность государства.

Библиография

1. Конституционный Суд Азербайджанской Республики. XVII Конгресс Конференции Европейских Конституционных Судов «Роль Конституционных Судов в правовой охране и применении конституционных принципов». [Электронный ресурс]. Режим доступа: /https://constcourt.ge/congress20152017/downloads//azerbaijan (дата обращения: 30.11.2021)

2. Копылов В.А. Информационное право. - Москва: Юрист, - 2004. - 512 с.

3. Лаврентьева М. Конституционно-правовой статус ребенка и особенности его реализации в РФ // – Москва, 2018. № 2. – с. 46- 56

4. Михайлов И.Г. Конституционно-правовое регулирование информационной сферы: автореф. дис… канд. юрид. наук. – Санкт-Петербург, 2001. – 25 с.

5. Тоффлер Э. Третья волна. – Москва, – 1999. – 800 с.

6. Шайкенов Н.А. Правовое обеспечение интересов личности: / автореф. дис… докт. юрид. наук / – Алма-Ата, 1992. – 56 с.

7. Information and documentation. Appraisal for managing records. ISO 2018: Available at: https://www.sis.se/api/document/preview/80007862/ (дата обращения: 18.11.2021)

Farzullayeva A.E.♦

DOI: 10.25108/2304-1730-1749.iolr.2021.65.73-79
UDC: 342.4

Threats to the digital sovereignty of the state

Abstract: The article is devoted to the study of threats to the digital sovereignty of the state. The conducted analysis allows in the process of further research to consider information sovereignty as the ability to technologically and legislatively ensure and protect the independence of the state and the constitutional rights of citizens in the information space from external threats. Information sovereignty includes the capabilities of the state in accordance with the Constitution and the entire national legal system, as well as international law independently and independently, in compliance

♦ **Farzullayeva Afat Elkhan** – dissertator of the Institute of Law and Human Rights of the ANAS (Azerbaijan). E-mail: afatgahramanova@gmail.com

with the balance of interests of the individual, society and the state, to determine and protect national interests in the information space and ensure the information security of the state.

Keywords: information; threat; state; digital sovereignty.

References

1. *Konstitutsionnyi Sud Azerbaijanskoyi Respubliki. 17 Kongress Konferetsii Evropeyiskikh Konstitutsionnykh Sudov* [Constitutional Court of Azerbaijan Republic. 17th Congress of the European Constitutional Courts. Role of the Constitutional Courts in legal protection and application of constitutional principles]. Available at: /https://constcourt.ge/congress 20152017/downloads//azerbaijan (accessed: 30.11.2021)

2. Kopylov V.A. *Informatsionnoe pravo* [Informational law]. Moscow, Yurist Publ., 2004, 512 p.

3. Lavrent'eva M. *Konstitutionno-pravovoyi status rebenka i osobennosti ego realizatsii v RF* [Constitutional legal status of a child and particularities its realization in RF]. Moscow, 2018. No. 2. P. 46- 56

4. Mikhailov I.G. *Konstitutsionno-pravovoe regulirovanie informatsionnoyi sfery*. Avtoref dis. kand. yurid. nauk [Constitutional legal regulation of the informational sfere. Abstract of PhD in Law Diss.]. S. Petersburg, 2001, 25 p.

5. Toffler E. *Tret'ya volna* [Third wave]. Moscow, 1999, 800 p.

6. Shaikenov N.A. *Pravovoe obespechenie interesov lichnosti*. Avtoref dis. dok. yurid. nauk [Legal supporting of an individual's interests. Abstract of Doctor of Law Diss.]. Almata, 1992, 56 p.

7. Information and documentation. Appraisal for managing records. ISO 2018. Available at: https://www.sis.se/api/document/preview/80007862/ 9accessed: 18.11.2021)