ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ
МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ (УНИВЕРСИТЕТ)
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

Лю Кирилл Алексеевич

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЕДИНОГО ЦИФРОВОГО ПРОСТРАНСТВА В ЕС И В ЕАЭС В УСЛОВИЯХ СОВРЕМЕННЫХ ТЕХНОЛОГИЧЕСКИХ ИЗМЕНЕНИЙ

Специальность 5.1.5. Международно-правовые науки

Диссертация на соискание ученой степени
кандидата юридических наук

Научный руководитель:
кандидат юридических наук, доцент
Торкунова Екатерина Анатольевна

Москва – 2025

Содержание:

Введение 3

Глава I. Теоретико-методологические основы исследования наднационального регулирования цифрового пространства в рамках современных интеграционных объединений 22

§ 1.1. Трансформация правового регулирования в цифровую эпоху 22

§ 1.2. Вызовы цифровой эпохи, стоящие перед наднациональным правовым регулированием региональных интеграционных объединений 27

§ 1.3. Основные направления наднационального регулирования общественных отношений в цифровой сфере 39

Глава II. Наднациональное регулирование цифрового пространства в рамках ЕС 55

§ 2.1. Развитие наднационального регулирования цифрового пространства в ЕС 55

§ 2.2. Особенности правового регулирования цифровой инфраструктуры и цифровой среды на уровне ЕС 74

§ 2.3. Особенности правового регулирования цифрового рынка и цифровых услуг на уровне ЕС 84

2.3.1. Наднациональное регулирование цифровых услуг 84

2.3.2. Наднациональное регулирование цифровых рынков 95

2.3.3. Наднациональное регулирование ИИ и криптоактивов в ЕС 105

Глава III. Проблемы и перспективы регулирования цифрового пространства на уровне ЕАЭС 113

§ 3.1. Особенности и основные направления регулирования цифрового пространства в рамках ЕАЭС 113

§ 3.2. Направления стратегического развития наднационального регулирования цифрового пространства в рамках ЕАЭС 128

Заключение 152

Список использованных источников и литературы 160

Введение

Актуальность выбранной для исследования темы. Необходимость исследования особенностей правового регулирования единого цифрового пространства в Европейском союзе (далее — ЕС) и в Евразийском экономическом союзе (далее — ЕАЭС), прежде всего, обусловлена последовательным увеличением роли современных информационно-коммуникационных технологий в общественной жизни, что особенно стало заметно в условиях глобальной пандемии COVID-19, сопряженной с ограничениями социальных взаимодействий в традиционных форматах.

Трансформация общественной жизни (ее нарастающая цифровизация) порождает принципиально новые вызовы для правового регулирования (в т.ч. наднационального). С увеличением роли информационно-коммуникационных технологий по-новому начали звучать проблемы обеспечения кибербезопасности, предоставления доступа к созданию и развитию информационно-коммуникационные технологии (далее — ИКТ) иностранным юридическим лицам, актуализировалась дискуссия о создании специальных антимонопольных требований, подлежащих применению в цифровой сфере. Также углубилась проблема создания эффективного правового регулирования обращения персональных (и неперсональных) данных в сетевом пространстве, защиты этих данных, их хранения и удаления (в т.ч. в рамках систем искусственного интеллекта). Дополнительные сложности возникли и в контексте нерешенных проблем с защитой интеллектуальной собственности и авторских прав в сети Интернет. Возросла и значимость формирования современной правовой базы в сфере кибербезопасности и защиты от кибертерроризма. Дополнительную актуальность получили проблемы правового противодействия распространению ложной и не соответствующей действительности информации в сети Интернет. С особенностями правового регулирования цифрового пространства тесно начали связываться вопросы защиты

окружающей среды (прежде всего, в контексте требований о климатической нейтральности и энергоэффективности объектов цифровой инфраструктуры)[1].

В целом круг вызовов для правового регулирования, связанных с широкомасштабной цифровизацией общественной жизни, настолько широк, что сегодня все чаще решение соответствующих проблем обеспечивается не по отдельности, а комплексно — в рамках правового регулирования цифрового пространства в целом. Так, на уровне ЕС подобное комплексное правовое регулирование в настоящее время принимает форму создания единого цифрового пространства интеграционного объединения.

На уровне ЕАЭС сегодня ведется деятельность по формированию наднациональных правовых основ единого цифрового пространства. Соответствующие положения содержатся в рамках дополнительных протоколов к Договору о Евразийском экономическом союзе[2] (в частности, в Протоколе об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза[3], которым устанавливаются общие особенности обмена неперсональными государственными данными в рамках ЕАЭС). Кроме того, в настоящее время в ЕАЭС реализуется Цифровая повестка ЕАЭС[4], которая предполагает формирование: 1) цифрового измерения интеграции

---

[1] Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. 2023. № 1. С. 12–25.

[2] Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014) // Официальный сайт Евразийской экономической комиссии http://www.eurasiancommission.org/, 05.06.2014.

[3] Приложение № 3 к Договору о Евразийском экономическом союзе. Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза [Электронный ресурс] // Режим доступа: https://docs.eaeunion.org/ru-ru/Pages/DisplayDocument.aspx?s=bef9c798-3978-42f3-9ef2-d0fb3d53b75f&w=632c7868-4ee2-4b21-bc64-1995328e6ef3&l=540294ae-c3c9-4511-9bf8-aaf5d6e0d169&EntityID=3610 (дата обращения: 14.03.2024).

[4] Заявление о цифровой повестке ЕАЭС [Электронный ресурс] // Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Pages/docs.aspx (дата обращения: 14.03.2024).

(электронный документооборот, наднациональные базы данных, межгосударственные цифровые сервисы и услуги); 2) цифровых рынков ЕАЭС; 3) цифровых инфраструктур и цифровых активов ЕАЭС[5].

Однако уровень интеграции в цифровой сфере в рамках ЕАЭС существенно ниже по сравнению со степенью интеграции в рамках ЕС. ЕАЭС в настоящее время находится лишь на стадии становления отдельных элементов единого цифрового пространства. Как следствие, опыт ЕС в соответствующей сфере может быть полезен для разработки и внедрения более эффективного наднационального регулирования как отдельных аспектов деятельности в цифровой среде, так и единого цифрового пространства в целом. В то же время стоит отметить, что в ЕС накоплен не только позитивный, но и негативный опыт в соответствующей сфере. Учет этого опыта представляет ценность для развития интеграции в рамках ЕАЭС.

Таким образом, в условиях современных технологических изменений возникают принципиально новые направления наднационального регулирования цифрового пространства, которые нуждаются в постоянном теоретическом осмыслении. Это предопределяет не только практическую, но и теоретическую актуальность выбранной для исследования темы.

Степень научной разработанности выбранной для исследования темы достаточно высока. В современной отечественной литературе существует большое количество трудов, посвященных общетеоретическим вопросам в сфере интеграционного права.

В частности, можно отметить работы таких авторов, как А.Х. Абашидзе[6], П.Н. Бирюков[7], В.В. Войников[8], Д.В. Галушко[9], Е.Н. Егорова[10],

---

[5] Общие подходы к формированию цифрового пространства Евразийского экономического союза в перспективе до 2030 года (Подготовлено ЕЭК в рамках выработки предложений по формированию цифрового пространства ЕАЭС) [Электронный ресурс] // Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Pages/docs.aspx (дата обращения: 14.03.2024).

А.Я. Капустина[11], Р.А. Касьянов[12], С.Ю. Кашкин[13], А.В. Клемин[14], Ю.М. Колосов[15], И.М. Лифшиц[16], А.А. Моисеев[17], А.А. Наку[18], Т.Н. Нешатаева[19],

---

[6] Право Европейского союза в 2 ч. / А. Х. Абашидзе [и др.]; под редакцией А. Х. Абашидзе, А. О. Иншаковой. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2024. 892 с.

[7] Бирюков М.М., Энтин Л.М., Энтин М.Л. Европейское право. Основы интеграционного права Европейского Союза. М.: Норма, 2023. 528 с.

[8] Войников В.В. Право Европейского Союза в практике Европейского Суда по правам человека // Международное правосудие. 2020. №1 (33). С. 50–66; Войников В. В., Энтина Е. Г., Энтин М. Л. Перспективы, потребности и подводные камни конституционализации ЕС и ЕАЭС // Полис. Политические исследования. 2019. № 4. С. 89-103; Войников В.В. Правовое регулирование информационных систем пространства свободы, безопасности и правосудия ЕС // Вестник Саратовской государственной юридической академии. 2019. № 4 (129). С. 99-111

[9] Галушко Д.В. Теория и практика правового регулирования интеграционных процессов в свете вызовов Брекзита: дис. … д-ра юрид. наук. М., 2023. 544 с.

[10] Егорова Е.Н. Перспективы перехода европейского союза к политическому союзу: договор, учреждающий конституцию для Европы // Идеи конституционализма в юридической науке: история и современность. Сборник материалов третьей международной научной конференции, посвященной памяти профессора В.М.Курицына. 2019. С. 67-81.

[11] Право Европейского союза: учебник для вузов / А. Я. Капустин [и др.]. Москва: Издательство Юрайт, 2022. 387 с.

[12] Касьянов Р.А. Обеспечение экономических прав и свобод человека и построение единого рынка финансовых услуг в Европейском союзе // Вопросы российского и международного права. 2019 Т. 9. №4. С. 152-161.

[13] Кашкин С. Ю. Право Европейского союза в 2 т. / С. Ю. Кашкин, А. О. Четвериков; отв. ред. С. Ю. Кашкин. 4-е изд., перераб. и доп. М.: Юрайт, 2024. 1647 с.; Интеграционное право в современном мире: сравнительно-правовое исследование / ред. С. Ю. Кашкин. Москва: Проспект, 2015. 412 с.

[14] Клемин А.В. Европейское право и Германия: баланс национального и наднационального. Европейское Сообщество, Германия, право: национальный консерватизм, коллизии и единство. Казань: Изд-во Казанск. ун-та, 2004. 588 с.

[15] Колосов Ю.М. О понятии европейского международного права // Российский ежегодник международного права. 2006. С. 194-198; Европейское международное право: Учебник / Ю.М. Колосов, Э.С. Кривчикова, Д.В. Иванов и др.; Отв. ред. Ю.М. Колосов, Э.С. Кривчикова, П.В. Савaськов. М.: Международные отношения, 2005. 408 с.

[16] Лифшиц И. М. Международное финансовое право и право Европейского союза: взаимодействие и взаимовлияние: монография. Москва: Юстицинформ, 2020. 548 с.; Лифшиц И. М. Проблема квалификации права Европейского Союза как правовой системы // Актуальные проблемы российского права. 2019. №11 (108). С. 153-162.

[17] Интеграционное правосудие: сущность и перспективы: Монография / С.Ю. Кашкин, П.А. Калиниченко, Я.С. Кожеуров, Е.Г. Моисеев; Отв. ред. С.Ю. Кашкин. М.: Норма: НИЦ ИНФРА-М, 2019. 112 с.

[18] Наку А.А. Таможенное право // Европейское право. Отрасли права Европейского Союза и Евразийского экономического союза: учебник / рук. авт. кол. и отв. ред. Л.М.Энтин, М.Л.Энтин. М.: Норма: ИНФРА-М, 2018. С. 15-70.

В.Л. Толстых[20], Н.Б. Топорнин[21], Е.А. Торкунова[22], Е.Т. Усенко[23], Л.М. Энтин[24], М.Л. Энтин[25] и др.

Непосредственно в сфере наднационального регулирования цифрового пространства стоит отметить коллективную монографию сотрудников МГИМО МИД России «The Platform Economy. Designing a Supranational Legal Framework»[26]. Также общим вопросам регулирования цифрового

---

[19] Нешатаева, Т. Н. Суд и право: евразийская интеграция: монография. Москва: Норма: ИНФРА-М, 2024. 336 с.; Нешатаева Т. Н. Интеграция и наднационализм // Вестник Пермского университета. Юридические науки. 2014. №2 (24). С. 243-248.

[20] Толстых В.Л. Размышления о евразийской интеграции // Sumus ubi sumus. Международное право XXI века: мир и безопасность, сотрудничество, права человека. Liber amicorum в честь профессора Л.П. Ануфриевой. М.: Проспект, 2016. С. 277-279.

[21] Топорнин Н.Б. Банковское право Европейского Союза и организационно-правовые основы функционирования Экономического и валютного союза / Н.Б.Топорнин // Европейское право. Отрасли права Европейского Союза и Евразийского Экономического Союза / И.В.Гудков и др.; под ред. Л.М.Энтина, М.Л.Энтина. М.: Норма, 2018. С. 156-190.

[22] Энтин М.Л., Энтина Е.Г., Торкунова Е.А. Сегодня и завтра ЕС сквозь призму правового инструментария углубления интеграции. Часть I // Современная Европа. 2019. №1. С. 27-37; Энтин М.Л., Энтина Е.Г., Торкунова Е.А. Сегодня и завтра ЕС сквозь призму правового инструментария углубления интеграции. Часть II // Современная Европа. 2019. №2. С. 39-49; Greater Eurasia: In Search of a Legal Order / У.Э. Батлер, М.Л. Энтин, Е.Г. Энтина, Е.А. Торкунова / Полис. Политические исследования. 2020. №4. С. 9-23.

[23] Курс международного права: Международно-правовые формы интеграционных процессов в современном мире. В 7-ми томах. Т. 7 / Бардина М.П., Войтович С.А., Колосов Ю.М., Кузнецов В.И., и др.; Отв. ред.: Усенко Е.Т. М.: Наука, 1993. 328 с.

[24] Европейское право. Основы интеграционного права Европейского союза и Евразийского экономического союза: учебник / рук. авт. кол. и отв. ред. Л.М. Энтин, М.Л. Энтин. М.: Норма: ИНФРАМ, 2018. 528 с.

[25] Энтин М.Л., Энтина Е.Г. Политическое и регуляторное обеспечение мировых интеграционных процессов: Усилия России, Китая, Индии, ЕС и США по обретению стратегической глубины в 2022–2023 годах: Научная монография / М.Л. Энтин, Е.Г. Энтина. Москва: Галактика, Издательский Дом «Зебра Е», 2023. 622 с.; Энтин М.Л. Перспективы, потребности и подводные камни конституционализации ЕС и ЕАЭС / М.Л. Энтин, Е.Г. Энтина, В.В. Войников // Полис. Политические исследования. 2019. №4. С. 89-103; Энтин М.Л., Войников В.В., Торкунова Е.А. Новый этап в институционально-правовом обустройстве пространства свободы, безопасности и правосудия ЕС // Московский журнал международного права. 2018. № 2. С. 102-114; Entin M.L. Difficult Choice of a Rational Approach to Regulating the Activities of Digital Platforms / M.L.Entin, E.A.Torkunova, S.O.Korogod // The Platform Economy. Palgrave Macmillan, Singapore, 2022. P. 253–269.

[26] The Platform Economy. Designing a Supranational Legal Framework / Editors: M.I. Inozemtsev, E.L. Sidorenko, Z.I. Khisamova. Palgrave Macmillan Singapore, 2022. 455 p.

пространства на интеграционном уровне посвящены статьи Е.С. Зиновьевой[27], И.М. Поповой[28], Э.В. Талапиной[29] и др.

В отечественной правовой литературе достаточно подробно исследованы вопросы, связанные с наднациональным регулированием отдельных сфер цифрового пространства, включая:

- вопросы кибербезопасности и информационной безопасности (А.Н. Бороздин[30], К.А. Ермак[31], Р. А. Касьянов[32] и др.);

- вопросы обращения персональных данных (С. Л. Ларионова[33], С. Г. Чубукова[34], А.Ю. Чурилов[35] и др.);

- вопросы обращения неперсональных данных (включая обращение таможенных данных) (А.М. Зуева[36], О.Б. Иванова[37], Ю.П. Кузякин[38], С.В. Мозер[39], С.Н. Ревина[40], А.Е. Шаститко[41] и др.);

---

[27] Зиновьева Е., Булва В. Цифровой суверенитет ЕС // Современная Европа. 2021. №2. С, 40-49; Зиновьева Е.С. Проблемы международного управления Интернетом в контексте цифрового суверенитета // Международная жизнь. 2020. Специальный выпуск. С. 133-137.

[28] Попова И.М. Проблемы реализации цифровой повестки ЕАЭС // Вестник международных организаций: образование, наука, новая экономика. 2021. №1. С. 127-141.

[29] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. №2 (254). С. 5-17.

[30] Бороздин А.Н., Коварда В.В. Анализ системы обеспечения защиты информации в процессе цифровизации ее оборота в рамках ЕАЭС в аспекте повышения экономической безопасности // Вестник Евразийской науки. 2020. Т. 12. № 4. С. 1-15.

[31] Ермак К.А. Информационная безопасность как элемент интеграции в рамках ЕАЭС // Социальные новации и социальные науки. 2023. №3 (12). С. 132-142.

[32] Касьянов Р. А. Международный опыт противодействия киберугрозам / Р. А. Касьянов // Российский следователь. 2023. № 6. С. 59-63.

[33] Ларионова С. Л. Методика защиты персональных данных с учетом требований регламента ЕС General Data Protection Regulation // Инновации и инвестиции. 2020. № 6. С. 198-205.

[34] Чубукова С. Г. Правовые проблемы обработки персональных данных в контексте COVID-19: опыт России и ЕС // Роль и значение права в условиях пандемии: Монография по итогам Международного онлайн-симпозиума / Под общей редакцией В.В. Блажеева, М. А. Егоровой. Москва: Общество с ограниченной ответственностью "Проспект", 2021. С. 52-62.

[35] Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Сибирское юридическое обозрение. 2019. №1. С. 29-35.

[36] Зуева А.М., Шайдуллова М.В. Цифровой транспортный коридор как новый элемент в организации таможенного контроля // NovaUm.Ru. 2018. № 13. С. 99–101.

- вопросы наднационального регулирования искусственного интеллекта (А.Ю. Марченко[42], А.Ж. Степанян[43] и др.);

- вопросы наднационального регулирования финансовых рынков в условиях цифровизации (Р.А. Касьянов[44]) и др.

Таким образом, можно констатировать, что степень научной разработанности выбранной для исследования темы в отечественной правовой науке достаточно высока. Однако она носит фрагментарный характер. Достаточно подробно исследован опыт ЕС в сфере наднационального регулирования цифрового пространства. В то же время степень научной разработанности вопросов регулирования цифрового пространства в ЕАЭС в настоящее время недостаточна. Наиболее подробно исследованы вопросы обращения неперсональных данных на уровне ЕАЭС (включая обращение таможенных данных и общие вопросы функционирования электронной таможни), в то время как другие направления регулирования цифрового пространства на уровне ЕАЭС в настоящее время получили свое освещение лишь в отдельных исследованиях.

---

[37] Иванова О.Б., Хапилин А.Ф., Хапилин С.А. Цифровая повестка ЕАЭС в контексте модернизации системы таможенного администрирования // Вестник Ростовского государственного экономического университета (РИНХ). 2020. № 1 (69). С. 157-163.

[38] Кузякин Ю.П., Мухин А.И. Цифровая трансформация таможенного контроля: состояние и перспективы // Юридическая наука. 2023. №8. С. 111-117.

[39] Мозер С.В., Секербаева Д.К. К вопросу о функционировании тематического блока «электронная таможня» в Евразийском экономическом союзе // Социально-политические науки. 2020. Т. 10. № 1. С. 49-59.

[40] Ревина С.Н., Лунева У.С. Вопросы таможенного регулирования в условиях развития интернет-торговли // МНИЖ. 2023. №4 (130). С. 1-5.

[41] Шаститко А.Е., Шпакова А.А. Регулирование трансграничного электронного документооборота в Евразийском экономическом союзе // Государственное управление. Электронный вестник. 2018. № 71. С. 242-269.

[42] Марченко А.Ю. Правовой анализ новейшего законодательства ЕС о применении технологий искусственного интеллекта: дис. … канд. юрид. наук. Москва, 2022. 208 с.

[43] Степанян А.Ж. Регламент Европейского Союза об искусственном интеллекте (Artificial Intelligence Act): первый взгляд на проект // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. № 7. С. 93-98.

[44] Касьянов, Р. А. Цифровизация как важный фактор регулирования российского финансового рынка и Союза рынков капитала ЕС / Р. А. Касьянов, М. А. Евдокимов // Право и цифровая экономика. 2022. № 4(18). С. 36-47; Касьянов, Р. А. Правовые основания цифровизации финансового сектора Европейского союза / Р. А. Касьянов // Банковское право. 2023. № 2. С. 49-58.

Объектом исследования являются общественные отношения, складывающиеся в рамках цифрового пространства и выступающие предметом регулирования на уровне интеграционных объединений.

Предметом исследования выступили положения интеграционных актов ЕС и ЕАЭС, международных договоров ЕАЭС, регулирующие общественные отношения в цифровом пространстве, а также иные официальные документы, акты Суда ЕС и Суда ЕАЭС в соответствующей сфере. Дополнительным предметом исследования послужили доктринальные теоретические модели регулирования цифрового пространства (и его отдельных элементов) на интеграционном уровне.

Цель исследования состоит в том, чтобы на основе сравнительно-правового анализа опыта ЕС и ЕАЭС выявить ключевые направления интеграционного регулирования цифрового пространства, наиболее актуальные подходы в соответствующей сфере. Для достижения данной цели в работе последовательно решается следующий ряд **задач:**

- выявить общие особенности и направления трансформации правового регулирования в цифровую эпоху;
- оценить вызовы цифровой эпохи, стоящие перед наднациональным правовым регулированием региональных интеграционных объединений;
- определить основные направления наднационального регулирования общественных отношений в цифровой сфере;
- проанализировать развитие наднационального регулирования цифрового пространства в ЕС;
- установить особенности правового регулирования цифровой инфраструктуры и цифровой среды на уровне ЕС;
- исследовать особенности правового регулирования цифрового рынка и цифровых услуг на уровне ЕС;

- выявить общие особенности и основные направления регулирования цифрового пространства в рамках ЕАЭС;
- определить направления стратегического развития интеграционного регулирования цифрового пространства в рамках ЕАЭС.

Научная новизна настоящего исследования обусловлена разработанной автором категоризацией основных направлений наднационального регулирования общественных отношений в цифровой сфере; авторской периодизацией развития наднационального регулирования цифрового пространства в ЕС; авторской категоризацией и оценкой основных направлений наднационального регулирования цифрового пространства в ЕАЭС; предложениями по совершенствованию правового режима внешней электронной торговли, закрепленного в Таможенном кодексе ЕАЭС (далее — ТК ЕАЭС) в конце 2023 г.

Теоретическая и практическая значимость. Теоретическая значимость исследования состоит в дополнении и расширении теоретических знаний в сфере особенностей наднационального регулирования цифрового пространства региональных интеграционных объединений в целом, а также особенностей наднационального регулирования отдельных групп общественных отношений, возникающих в цифровой среде (в частности, к таким группам могут быть отнесены общественные отношения в сфере передачи, использования, хранения и удаления персональных данных; в сфере оборота неперсональных данных; в сфере обеспечения кибербезопасности; в сфере создания и функционирования цифровой (в том числе облачной) инфраструктуры; в сфере оказания цифровых услуг и продажи цифровых товаров; в сфере организации функционирования цифровых рынков и т.д.). Кроме того, с теоретической точки зрения, результаты и выводы исследования могут быть полезны для расширения научных знаний о динамике правового регулирования цифрового пространства в ЕС и в ЕАЭС. Практическая значимость работы

преимущественно сконцентрирована на формировании предложений по разработке, внедрению и совершенствованию наднационального регулирования общественных отношений, возникающих в цифровом пространстве на уровне ЕАЭС.

Теоретическую основу исследования составили концепции и теории интеграционного права. В частности, были использованы общие подходы к пониманию интеграционного права, его особенностей и структуры, разработанные Л.М. Энтиным[45] и М.Л. Энтиным[46], а также В.В. Войниковым[47], Е.Н. Егоровой[48], Р.А. Касьяновым[49], А.А. Наку[50], Н.Б. Топорниным[51], Е.А. Торкуновой[52] и др. Также теоретическую основу исследования составили концепции отечественных и зарубежных авторов, описывающие общие особенности правового регулирования цифровой сферы

[45] Бирюков М.М., Энтин Л.М., Энтин М.Л. Европейское право. Основы интеграционного права Европейского Союза. М.: Норма, 2023. 528 с.
[46] Энтин М.Л., Энтина Е.Г., Торкунова Е.А. Сегодня и завтра ЕС сквозь призму правового инструментария углубления интеграции. Часть I // Современная Европа. 2019. №1. С. 27-37; Энтин М.Л., Энтина Е.Г., Торкунова Е.А. Сегодня и завтра ЕС сквозь призму правового инструментария углубления интеграции. Часть II // Современная Европа. 2019. №2. С. 39-49.
[47] Войников В. В., Энтина Е. Г., Энтин М. Л. Перспективы, потребности и подводные камни конституционализации ЕС и ЕАЭС // Полис. Политические исследования. 2019. № 4. С. 89-103; Войников В.В. Право Европейского Союза в практике Европейского Суда по правам человека // Международное правосудие. 2020. №1 (33). С. 50–66.
[48] Егорова Е.Н. Перспективы перехода европейского союза к политическому союзу: договор, учреждающий конституцию для Европы // Идеи конституционализма в юридической науке: история и современность. Сборник материалов третьей международной научной конференции, посвященной памяти профессора В.М.Курицына. 2019. С. 67-81.
[49] Касьянов, Р. А. Правовые основания цифровизации финансового сектора Европейского союза // Банковское право. 2023. № 2. С. 49-58.
[50] Наку А.А. Таможенное право // Европейское право. Отрасли права Европейского Союза и Евразийского экономического союза: учебник / рук. авт. кол. и отв. ред. Л.М.Энтин, М.Л.Энтин. М.: Норма: ИНФРА-М, 2018. С. 15-70.
[51] Топорнин Н.Б. Банковское право Европейского Союза и организационно-правовые основы функционирования Экономического и валютного союза / Н.Б.Топорнин // Европейское право. Отрасли права Европейского Союза и Евразийского Экономического Союза / И.В.Гудков и др.; под ред. Л.М.Энтина, М.Л.Энтина. М.: Норма, 2018. С. 156-190.
[52] Greater Eurasia: In Search of a Legal Order / У.Э. Батлер, М.Л. Энтин, Е.Г. Энтина, Е.А. Торкунова / Полис. Политические исследования. 2020. №4. С. 9-23.

в условиях современных технологических изменений. Кроме того, в качестве теоретических основ исследования были использованы концепции зарубежных исследователей, содержащие в себе теоретические модели наднационального регулирования цифровой сферы в целом и отдельных направлений цифровой деятельности в рамках ЕС.

Методология и методы исследования. Метанаучной основой (общим методологическим направлением) исследования выступила материалистическая диалектика. Ключевую роль сыграл закон перехода количественных изменений в качественные, в соответствии с которым исследовались процессы постепенного нарастания количества общественных отношений, завязанных на цифровую сферу, итогом чего стало формирование цифрового пространства. Следуя за изменением общественных отношений, меняется и интеграционное правовое регулирование: на первых этапах регулируются отдельные общественные отношения, возникающие в цифровой сфере (в сфере электронной торговли, обращения цифровых данных и др.); а на более поздних этапах формируется комплексная система интеграционного регулирования цифрового пространства в целом.

Среди общенаучных методов в исследовании были применены: анализ (для выявления составляющих интеграционного регулирования цифрового пространства); синтез (для формирования выводов о системе интеграционного регулирования цифрового пространства); индуктивно-дедуктивный метод (посредством которого отдельные практики интеграционного регулирования были обобщены в рамках укрупненных направлений); системный метод (позволивший рассматривать интеграционное регулирование цифровой сферы как систему); структурно-функциональный метод (на основе которого были определены состав и функции инструментов интеграционного регулирования цифрового пространства).

К специальным научным методам, использованным в исследовании, относятся: историко-правовой метод (на основе которого были выявлены ключевые этапы развития интеграционного регулирования цифрового пространства в ЕС); сравнительно-правовой метод (использованный для сопоставительного анализа интеграционного регулирования цифрового пространства в ЕС и ЕАЭС); метод системного анализа права (позволивший установить системную взаимосвязь инструментов и форм интеграционного регулирования цифрового пространства в ЕС и ЕАЭС); формально юридический метод (примененный для анализа содержания интеграционных актов ЕС и ЕАЭС); метод анализа правоприменительной практики (был использован для анализа практики Суда ЕС и Суда ЕАЭС в цифровой сфере); метод правового моделирования (был применен для формулировки предложений по внесению изменений в ТК ЕАЭС в части внешней электронной торговли).

Нормативная основа исследования представлена наднациональными актами ЕС и ЕАЭС, посредством которых на интеграционном уровне осуществляется регулирование общественных отношений в цифровой сфере.

Эмпирическая основа исследования включает в себя материалы правоприменительной практики Суда ЕС и Суда ЕАЭС, а также официальные документы указанных интеграционных объединений, включая стратегии, рабочие документы, выступления и заявления официальных лиц.

Положения, выносимые на защиту:

1. Наднациональное регулирование цифрового пространства по критерию предмета регулирования подразделяется на три основных направления: 1) наднациональное регулирование порядка обращения данных в цифровом пространстве (включая регулирование обращения персональных и неперсональных данных, официальной государственной информации; а также регулирование цифровых публичных закупок и цифровой таможенный контроль); 2) наднациональное регулирование единых (общих) цифровых

рынков (регулирование цифровых услуг, конкуренции на цифровых рынках, деятельности цифровых компаний, искусственного интеллекта, криптоактивов, цифровых финансов, а также защита интеллектуальной собственности и авторских прав в цифровом пространстве); 3) наднациональное регулирование цифровой безопасности (противодействие киберпреступности и кибертерроризму, обеспечение безопасности и защищенности цифровой инфраструктуры, экологическая безопасность цифровой инфраструктуры). Приведенные три направления охватывают собой все сферы интеграционного регулирования цифрового пространства на современном этапе. Именно по данным направлениям должно развиваться интеграционное регулирование цифрового пространства в ЕАЭС.

2. Наднациональное регулирование цифровых услуг в правопорядке ЕС осуществляется на основе четырех правовых режимов: 1) правовой режим первичного права ЕС; 2) правовой режим услуг информационного общества; 3) правовой режим посреднических цифровых услуг; 4) правовой режим услуг основной цифровой платформы. Эти режимы выстроены иерархически по принципу от общих норм права к специальным.

- Общий правовой режим первичного права ЕС предполагает распространение на цифровые услуги правового режима права на получение информации. Он применяется, если отсутствует иное (специальное) регулирование.

- Особый правовой режим услуг информационного общества распространяется на возмездные цифровые услуги, которые не имеют материального содержания и предоставляются по индивидуальному запросу заказчика дистанционно посредством цифровых средств передачи данных без использования физических цифровых носителей и без присутствия исполнителя и заказчика одновременно в одном месте.

- Специальный правовой режим посреднических цифровых услуг распространяются на посреднические цифровые услуги: «просто проводник»

(*mere conduit*), «кэширование» (*caching*) и «хостинг» (*hosting*). Посреднические цифровые услуги выступают в качестве подвида услуг информационного общества.

- Квалифицированный правовой режим услуг основной цифровой платформы (правовой режим цифровых привратников) распространяется на посреднические цифровые услуги, в рамках которых обеспечивается онлайн-взаимодействие между конечными потребителями (конечными пользователями цифровых услуг) и субъектами предпринимательской деятельности (бизнес-пользователями услуг основной платформы).

3. Специальный правовой режим посреднических цифровых услуг по критерию содержания предоставляемых услуг дифференцирован на правовые режимы отдельных видов посреднических цифровых услуг, системы которых построена по принципу поэтапного усложнения и дополнения: 1) универсальный правовой режим – набор ограничений, обязанностей и требований к организации предоставления цифровых посреднических услуг, который распространяется на все цифровые посреднические услуги; 2) правовой режим хостинга – дополнительный набор ограничений, обязанностей и требований, распространяющийся на поставщиков цифровых услуг типа «хостинг»; 3) правовой режим онлайн-платформ – набор особых требований, предъявляемых к организации деятельности онлайн-платформ; 4) специальный правовой режим онлайн-платформ – набор специальных требований, соблюдение которых является обязательным для онлайн-платформ, посредством которых обеспечивается онлайн-торговля с участием потребителей; 5) правовой режим особо крупных онлайн-платформ и онлайн-поисковиков – данный режим подлежит применению к цифровым посредникам, деятельность которых оказывает влияние на предоставление цифровых услуг на системном уровне и несет в себе системные риски для цифрового пространства.

4. Квалифицированный правовой режим услуг основной цифровой платформы (квалифицированный правовой режим цифровых привратников) включает в себя четыре группы обязанностей, налагаемых на цифровых привратников: 1) обязанности цифровых привратников в части их взаимодействия с конечными пользователями (преимущественно связаны с обработкой и использованием их персональных данных); 2) обязанности цифровых привратников по отношению к бизнес-пользователям (преимущественно сводятся к установлению свободного сотрудничества бизнес-пользователей с конкретным поставщиком услуг основной цифровой платформы, а также предполагают установление прозрачных правил рекламирования товаров и услуг на основной цифровой платформе); 3) антимонопольные требования к цифровым привратникам (предусматривают недопустимость недобросовестной конкуренции, предотвращение рисков монополизации отдельных рынков цифровых услуг со стороны крупных цифровых привратников; необходимость обеспечения свободного использования стороннего программного обеспечения на основной цифровой платформе); 4) обязанности в сфере ежегодной отчетности о порядке обращения с персональными данными и о выполнении требований the Digital Markets Act (далее – DMA). Совокупное действие отмеченных групп обязанностей формирует комплексный квалифицированный правовой режим, в рамках которого обеспечивается регулирование основных точек риска в деятельности крупных цифровых компаний. Дифференциация обязанностей таких компаний может быть учтена при совершенствовании интеграционного регулирования цифрового пространства на уровне ЕАЭС.

5. Развитие интеграционного регулирования цифрового пространства в ЕАЭС строится на началах, противоположных целям ЕС в соответствующей сфере. В отличие от ЕС, в ЕАЭС приоритет закреплен за национальными интересами государств-членов. Все ключевые акты и стратегические документы, обеспечивающие формирование общего цифрового пространства

в рамках ЕАЭС, подчиняются, в первую очередь, национальным интересам государств-членов ЕАЭС и национальным стратегиям в соответствующей сфере. На наднациональном уровне могут осуществляться лишь шаги по координации действий государств-членов в цифровой сфере и по устранению барьеров на общих рынках ЕАЭС. Имплементация наднациональных положений осуществляется на уровне государств-членов, что предоставляет им дополнительную возможность для гибкой интеграции в цифровой сфере.

6. Среднесрочное развитие интеграционного регулирования цифрового пространства в ЕАЭС должно предполагать следующие основные шаги:

- Разработка интеграционных стандартов для гармонизации законодательства государств-членов ЕАЭС в сфере обращения персональных данных (в том числе, с учетом опыта ЕС при принятии GDPR) и в сфере обеспечения кибербезопасности (в т.ч. с учетом положения Директивы NIS 2).

- Расширение интеграционных основ защиты интеллектуальной собственности и авторских прав в цифровом пространстве путем принятия международных договоров между членами ЕАЭС, предусматривающих обязательства по разработке национального законодательства о выявлении и блокировании цифрового контента, нарушающего авторские права, с возможностью установления переходного периода для исполнения данных обязательств и возможностью установления отдельных изъятий государствами-членами ЕАЭС. Для структурирования обязательств государств-членов в части совершенствования национального законодательства может быть использована дифференциация обязательств поставщиков посреднических цифровых услуг по аналогии с DSA.

- Разработка интеграционных основ для координации и согласования законодательства государств-членов ЕАЭС в сфере защиты конкуренции на цифровых рынках и рынках цифровых услуг. В качестве позитивного опыта

можно использовать четыре группы обязательств цифровых привратников, закрепленных в DMA.

При этом передача вопросов обеспечения кибербезопасности на наднациональный уровень в настоящее время не видится возможной. Создание общих цифровых рынков в рамках ЕАЭС в настоящее время видится нецелесообразным.

7. Проект наднационального регулирования внешней (с участием резидентов третьих стран) электронной торговли в виде Протокола о внесении изменений в Таможенный кодекс ЕАЭС[53] характеризуется рядом системных проблем:

- отсутствует легальное определение электронной торговли, что влечет за собой пробельность правового режима внешней электронной торговли;

- сделки купли-продажи товаров электронной торговли не могут заключаться между физическими лицами[54]. На уровне текста законодательных новелл ТК ЕАЭС не предусмотрена возможность ИП и самозанятым пользоваться правовым режимом внешней электронной торговли в качестве продавцов;

- прямой запрет на использование товаров электронной торговли в коммерческой деятельности, закрепленный в ч. 2 ст. 309.1 будущей редакции ТК ЕАЭС, на практике влечет за собой фактическую невозможность ИП и самозанятым приобретать товары электронной торговли для коммерческой деятельности (т.е. выступать в качестве покупателей товаров электронной торговли)[55];

---

[53] Протокол о внесении изменений в Договор о Таможенном кодексе Евразийского экономического союза от 11 апреля 2017 года (Санкт-Петербург, 25 декабря 2023 года). [Электронный ресурс]. URL: https://www.alta.ru/tamdoc/23bn0196/ (дата обращения: 26.09.2024).

[54] Если обе стороны сделки являются физическими лицами, несмотря на использование маркетплейса (электронной торговой площадки) в качестве информационного посредника, приобретенные товары не будут квалифицироваться в качестве товаров электронной торговли.

[55] Ни иностранный продавец (поставщик) товаров электронной торговли, ни оператор электронной торговли не несут ответственность за реализацию товаров физическим

- не определен ряд важных обязанностей и сфер ответственности операторов электронной торговли. Однако введение в правовое поле ЕАЭС принципиально новой категории «оператор электронной торговли» неизбежно требует ее конкретизации.

8. Было разработано легальное определение электронной торговли, которое видится необходимым к закреплению в ТК ЕАЭС. Под электронной торговлей необходимо понимать совокупность информационно-коммуникационных технологий, сервисов, а также обеспечивающих программно-аппаратных средств, посредством которых обеспечивается функционирование цифровых онлайн-ресурсов (сайтов в сети Интернет, мобильных приложений и иных), предназначенных для осуществления дистанционного заключения договоров купли-продажи или поставки товаров.

Степень достоверности результатов исследования подтверждается использованием релевантной теоретико-методологической базы, а также широтой привлеченного нормативного и эмпирического материала, опора на который позволила подробно исследовать общие подходы и отдельные особенности наднационального регулирования цифрового пространства в ЕС и в ЕАЭС.

Апробация результатов исследования была осуществлена в ходе обсуждений работы на кафедре интеграционного права и прав человека МГИМО МИД России. Кроме того, результаты настоящего исследования были апробированы в рамках статей, опубликованных в изданиях,

---

лицам, которые впоследствии будут использовать их в коммерческой деятельности. Именно ИП или самозанятый при приобретении для коммерческой деятельности товаров на отечественных маркетплейсах будет обязан проверять, по итогам какой именно таможенной процедуры они реализуются на маркетплейсах. В условиях отсутствия публично достоверной информации обо всех таможенных операциях подавляющее большинство товаров на отечественных маркетплейсах, реализуемых иностранными резидентами, окажутся официально недоступны для ИП и самозанятых под угрозой привлечения их к юридической ответственности (в виде доначисления таможенных платежей и привлечения виновных лиц к ответственности за уклонение от уплаты таможенных платежей).

рецензируемых Высшей аттестационной комиссией при Министерстве образования и науки Российской Федерации.

1. Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. – 2022. – № 1. – С. 61–75[56].

2. Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. – 2023. – № 1. – С. 12–25[57].

3. Лю К.А. Новый порядок регулирования внешней электронной торговли в ЕАЭС: новеллы таможенного законодательства // Инновации и инвестиции. – 2024. – № 2. – С. 69–74[58].

4. Лю К.А. Основные направления международно-правового и наднационального регулирования цифрового пространства в рамках ЕАЭС на современном этапе // Право и управление. XXI век. – 2024. – Т. 20. № 1. – С. 84–91[59].

По **структуре** работа состоит из введения, трех глав, разделенных на восемь параграфов, заключения и списка использованных источников и литературы.

---

[56] Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. 2022. № 1. С. 61–75.

[57] Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. 2023. № 1. С. 12–25.

[58] Лю К.А. Новый порядок регулирования внешней электронной торговли в ЕАЭС: новеллы таможенного законодательства // Инновации и инвестиции. 2024. № 2. С. 69–74.

[59] Лю К.А. Основные направления международно-правового и наднационального регулирования цифрового пространства в рамках ЕАЭС на современном этапе // Право и управление. XXI век. 2024. Т. 20. № 1. С. 84–91.

Глава I. Теоретико-методологические основы исследования наднационального регулирования цифрового пространства в рамках современных интеграционных объединений

§ 1.1. Трансформация правового регулирования в цифровую эпоху

Цифровизация, наряду с глобализацией, является одним из ключевых трендов третьего тысячелетия, которые бросают вызов устоявшимся теоретическим конструкциям, социальным институтам и сложившимся практикам общественных отношений. Развитие информационных, а затем и цифровых технологий влечет за собой комплексную цифровую трансформацию социально-экономических систем, и государства с присущими им нормативными системами (правопорядками) здесь не являются исключением. Информационное общество[60] является основной предпосылкой социальных и правовых изменений, которые будут углубляться по мере дальнейшего формирования цифрового пространства как новой, виртуальной по своей сути, реальности.

Вкратце охарактеризуем эволюцию, которую претерпело государственное управление и правопорядок под влиянием информационно-коммуникационных и цифровых технологий. Выделение определенных этапов этой эволюции позволит уяснить и содержание указанных процессов.

Сразу после появления цифровых технологий[61] как на микроуровне (в рамках отдельных предприятий), так и на макроуровне (в рамках государственных органов) информация, содержащаяся на аналоговых или бумажных носителях, стала постепенно переводиться в машиночитаемую форму. Эти процессы были названы оцифровкой (англ. digitization), поскольку происходил перевод информации в компьютерный двоичный код (при сохранении прежних оригиналов, что вызывало дублирование

---

[60] Уэбстер Ф. Теории информационного общества / Под ред. Е. Л. Вартановой. М.: Аспект Пресс, 2004. 400 с.

[61] В рамках настоящего исследования под цифровыми технологиями будет пониматься электронные инструменты, системы, устройства и ресурсы, с помощью которых создаются, хранятся и обрабатываются цифровые данные.

документооборота). Основная цель процесса оцифровки — это оптимизация хранения данных, их обработки и передачи. Однако принципиально важно отметить, что качественных, содержательных изменений самой информации и отношений по ее использованию на данном этапе не происходило[62].

Следующий, более глубокий этап проникновения информационно-коммуникационных и цифровых технологий в деятельность государственных институтов стал обозначаться термином «цифровизация». На данном этапе информация уже не просто переводилась в машиночитаемый формат, а организовывалась в рамках новых продуктов и целых систем. Профессор Ю.И. Грибанов указывает на то, что основной идеей данного этапа стала «автоматизация управленческих процессов»[63], необходимая для повышения интенсивности информационного обмена между ключевыми элементами системы государственного управления (межведомственный обмен, различные формы коммуникации по линии «государство–граждане», включая предоставление публичных услуг). Именно на этом этапе в научный оборот был внедрен термин «электронное правительство», подразумевающий сервисную ориентацию государства, трансформацию привычного взаимодействия между государственными органами и населением.

Наконец, современный этап, обозначаемый термином «цифровая трансформация», описывает наиболее развитую стадию внедрения цифровых технологий в управленческие процессы. В отличие от двух предыдущих этапов, цифровая трансформация влечет за собой не просто смену формы предоставления данных или обеспечение автоматического обмена информации при помощи цифровых технологий, но появление новых форм коммуникации, принципиальное изменение внутренних и внешних взаимодействий, которые могут серьезно изменить самые фундаментальные

---

[62] Гончаренко Л.С. Цифровая экономика как фактор социально-экономической трансформации России // Вестник ЧелГУ. 2019. №3 (425). С. 43-49.

[63] Грибанов Ю.И. Цифровая трансформация социально-экономических систем на основе развития института сервисной интеграции: дис. … доктора эконом. наук. СПб., 2019. С. 14.

основы современной системы государственного управления. Содержание базовых понятий и устоявшихся концепций («государство», «право», «суверенитет» и т.п.) тоже может подвергнуться полному или частичному пересмотру под влиянием всепроникающих цифровых технологий.

В схематичном виде эволюция внедрения информационно-коммуникационных и цифровых технологий в практику социально-экономических систем представлена на Рисунке 1.

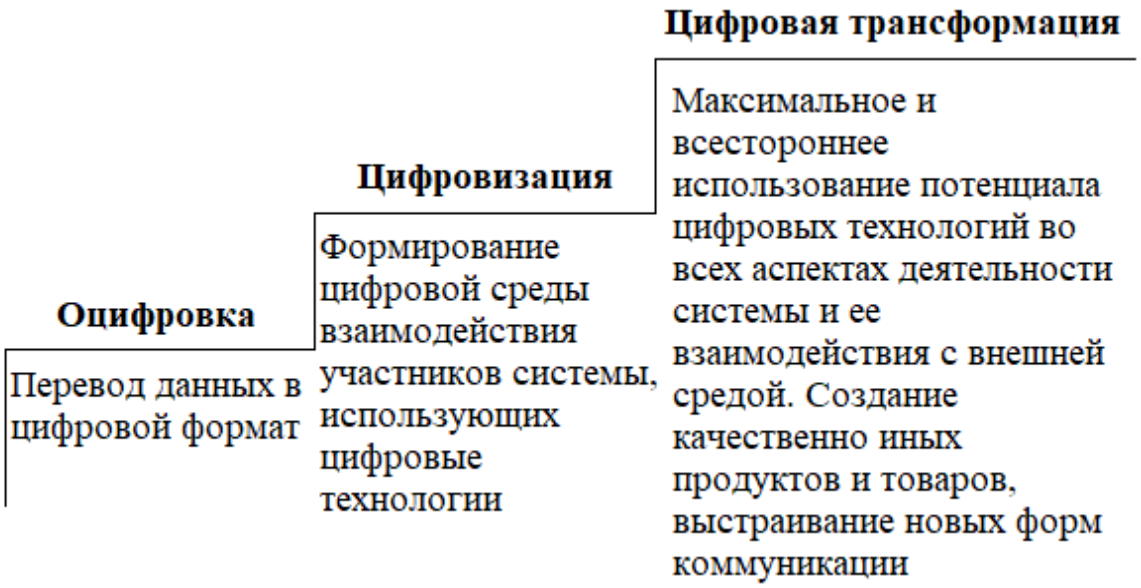


Рисунок 1. Уровни (этапы) внедрения цифровых технологий в социально-экономические системы[64]

Под цифровой трансформацией в настоящем исследовании предлагается понимать два ключевых взаимосвязанных аспекта. Во-первых, это технико-технологический процесс внедрения цифровых технологий в различные сферы экономической и социальной жизни, оцифровки данных и других ресурсов. Во-вторых, это организационный (по своей сути) процесс создания сервисных платформ, в рамках которых интегрируются различные цифровые технологии[65]. Именно в первом значении термин «цифровая трансформация» влечет за собой определенные риски, вызовы и

[64] Составлено автором.
[65] Грибанов Ю.И. Указ. соч. С. 7.

возможности, которые предопределяют появление в праве принципиально новых подходов к регулированию информационных отношений в обществе.

Разумеется, столь серьезные трансформации в экономике не могут не влиять на политическую и социальную сферы. Э.В. Талапина иллюстрирует тезис о принципиальной значимости цифровой трансформации для правовой науки, приводя классическое определение права как «совокупности норм, регулирующих отношения, складывающиеся между субъектами по поводу определенного объекта». Она указывает на то, что деконструкции могут быть подвергнуты такие элементы данного определения, как:

- субъекты права (проблема анонимности в Интернете, виртуальные личности, «цифровая смерть», боты, искусственный интеллект и т.п.);
- объекты права (появление цифровых объектов интеллектуальной собственности, регулирование информации в Сети, появление новых технологий и проблема применения к ним классических правовых конструкций и т.п.);
- действия субъектов по поводу объектов, т.е. правоотношения (появление новых форматов поведения, выражения воли, что имеет значение для гражданского, уголовного, административного и иных отраслей права)[66].

Можно заметить, что цифровая трансформация действительно затрагивает практически все ключевые для права категории. Это означает, что на более высоком уровне абстракции можно логически прийти к пониманию того факта, что Интернет сформировал особую, параллельную виртуальную реальность, которая в настоящей работе будет обозначаться термином «цифровое пространство». Именно в этом пространстве не только появляются новые субъекты, новые объекты и новые форматы взаимоотношений между ними, но и трансформируются привычные отношения между «классическими» субъектами и объектами права.

---

[66] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. №2 (254). С. 5-17.

Формирование новых общественных отношений, новых субъектов и объектов с неизбежностью требует включения их в предмет правового регулирования. Иными словами, перед государством и правом встает задача адекватного воздействия на эти отношения с максимально полезными социально-политическими эффектами. Возникают три ключевых вопроса: вопрос объекта (что регулировать?); вопрос методов (как регулировать?); вопрос субъекта (кому и на каком уровне регулировать?).

На более прикладном уровне заметно, что наиболее явными точками реагирования на вызовы и риски цифровой эпохи является несколько направлений: это регулирование контента, т.е. порядка обращения различной информации; регулирование инфраструктуры и технологий; охрана существующих отношений от особого рода угроз (киберугроз). Не меньшее значение имеет и регулирование уже устоявшихся сфер общественных отношений, которые видоизменяются под влиянием цифровых технологий (телекоммуникации, электронная торговля, электронное правительство и т.п.).

Сегодня государства и наднациональные объединения с неизбежностью включаются в технологическую гонку для обеспечения лидерства в формирующейся глобальной «экономике знаний»[67]. В этих условиях особое значение приобретает концепция «цифрового суверенитета» — самодостаточности отдельного государства или интеграционного объединения в цифровом сегменте, его контроле над ключевыми технологиями и данными. В этой связи как отдельные государства, так и интеграционные объединения (наиболее ярким примером здесь является ЕС) в целом объявляют курс на снижение зависимости от импорта цифровых технологий и сопутствующего оборудования, что рассматривается как путь к

[67] Foundations of the knowledge economy: innovation, learning, and clusters. Westeren, Knut Ingar. Cheltenham, UK: Edward Elgar. 2012. 296 p.

«стратегической автономии в цифровой сфере»[68]. Эта автономия тесно связана и с другой ключевой проблемой современности — кибербезопасностью. Более подробно данные аспекты будут затронуты в следующих главах настоящей работы.

§ 1.2. Вызовы цифровой эпохи, стоящие перед наднациональным правовым регулированием региональных интеграционных объединений

Сегодня каждое государство стремится урегулировать цифровое пространство как особую сферу «виртуальной реальности». По мере того, как одни общественные отношения приобретают дополнительное измерение за счет цифрового пространства, а другие отношения в принципе появляются как таковые благодаря развитию цифровых технологий, государства не могут игнорировать эти процессы. Экстерриториальный характер Сети превращает цифровое пространство в сферу конкуренции разных государств, ставя определенные вызовы перед классическими концепциями суверенитета.

Так, еще со времен эпохи Просвещения было признано, что суверенитет есть проявление власти, абсолютно самостоятельной в отношении определенной территории, определенного круга людей и вещей[69]. Независимость, отсутствие другого, равного суверену субъекта, влечет за собой признание за государственной властью абсолютного характера.

Таким образом, говоря о государственном суверенитете в рамках вестфальской системы международных отношений, мы всегда имеем в виду юридическое и властное верховенство суверена внутри страны (на определенной территории в отношении определенного населения), независимость страны на международной арене. Именно наличие суверенитета позволяет государствам независимо от внешних субъектов реализовывать собственную модель законодательной, исполнительной,

---

[68] См.: Digital sovereignty for Europe. European Parliament. EPRS Ideas Paper: Towards a more resilient EU, 2020. P. 16.

[69] Боден Ж. Метод легкого познания истории / под ред. М. С. Бобковой. М.: Наука, 2000. С. 15.

судебной власти, не отдавая какие-либо из своих полномочий другим государствам или международным организациям (за исключением добровольного делегирования определенных групп полномочий на международный или наднациональный уровень управления).

Повсеместное распространение Интернета в начале 1990-х гг. поставило серьезные вопросы о том, может ли быть урегулировано экстерриториальное коммуникативное пространство? Каким образом и кем именно может осуществляться подобная регуляция? Длительное время государства воздерживались от серьезных попыток вмешиваться в функционирование глобальной сети, благодаря чему Интернет оказывался «пространством максимальной свободы», стихийного взаимодействия пользователей. Активно рассматривались вопросы международного регулирования Интернета, распределения доменных имен, размещения серверов и т.п., однако в подавляющем большинстве государств не предпринималось серьезных попыток самостоятельно, в одностороннем порядке регулировать стихийно складывающиеся отношения в сетевом пространстве (т.е. реализовывать здесь суверенные полномочия).

В 2013 г. сотрудник Агентства национальной безопасности США Э. Сноуден обнародовал информацию о тотальной слежке правительства США и правительств ряда других государств за пользователями телефонной связи и Интернета. Всеобъемлющий характер контроля за данными, составляющими основу частной жизни человека, вызвал серьезные дискуссии относительно того, насколько государства могут быть автономны в защите «своего» сегмента информационного пространства, т.е. насколько они способны обеспечить свой суверенитет в «виртуальной реальности»[70].

В первую очередь, предметом данных дискуссий стала возможность закрывать уязвимости в сетевой инфраструктуре, обеспечивать защиту технологий, обеспечивающих функционирование национального сегмента

[70] Tréguer F. Intelligence reform and the Snowden paradox: The case of France // Media and Communication. 2017. №5 (1). P. 17–28

Интернета. Мощные IT-гиганты (Google, Amazon, Facebook/Meta и др.) перестали рассматриваться как внегосударственные, глобальные игроки: процедуры сбора, обработки, хранения, анализа персональных данных пользователей интернет-сервисов стали рассматриваться как уязвимость, которая может быть использована иностранными (в первую очередь, американскими) спецслужбами во внешнеполитических и разведывательных целях. «Нейтральность» Интернета как продукта и драйвера глобализации была совершенно справедливо поставлена под сомнение. В условиях обострившейся геополитической конкуренции о «цифровом суверенитете» задумались такие страны, как Россия и Китай, однако в последние годы страны ЕС тоже озабочены проблемами информационной безопасности, угрозы которой видятся, в том числе, в зависимости от иностранных объектов инфраструктуры и иностранных же технологий[71].

Выход вопросов регулирования цифрового пространства в топ политической и законотворческой повестки дня вызвал к жизни такой термин, как «цифровой империализм», которым стало обозначаться текущее положение американских IT-гигантов, посредством которых США получают возможность контролировать информационные потоки по всему миру, включая движение персональных данных более миллиарда людей. Попытки переломить статус-кво в указанной сфере (особого успеха здесь добился, например, Китай, создав независимую цифровую экосистему) вызвали встречную критику и были охарактеризованы как «цифровой протекционизм», препятствующий глобализации как естественному ходу истории и прогресса. Между двумя крайностями необходим баланс, гарантирующий как цифровой суверенитет, так и сохранение Интернета в

[71] Creemers R. China’s Conception of Cyber Sovereignty / in: D. Broeders & B. Berg (Eds.), Governing Cyberspace: Behavior, Power and Diplomacy. Rowman&Littlefield, 2020. P. 432.

качестве уникального коммуникативного пространства, не разделенного государственными границами[72].

Примечательно, что на уровне актов стратегического планирования большинство государств рассматривает меры по регулированию цифрового пространства и локализации объектов сетевой инфраструктуры не только в контексте национальной безопасности (в ее информационном аспекте), но и в контексте развития экономического и промышленного потенциала, инновационной политики, стимулирования научно-технического прогресса[73]. Действительно, сегодня уже с уверенностью можно констатировать, что XXI век станет веком цифровых технологий, и уровень развития этих технологий, степень контроля над ними являются важным фактором в глобальной экономической конкуренции. «Четвертая промышленная революция» может стать серьезным вызовом для текущего геоэкономического порядка; новая конфигурация сил на глобальном рынке напрямую зависит от того, какое государство сможет обеспечить лидирующие позиции в IT-индустрии и должный уровень информационной безопасности.

На это обращают внимание не только такие страны, как Россия, Китай, Индия и другие государства, озабоченные стимулированием собственного технологического роста и независимости от иностранных сервисов и технологий, но и государства – члены ЕС. В последние годы европейские эксперты все чаще указывают на то, что ЕС не сможет стать глобальным субъектом в формирующемся миропорядке, если не обеспечит резкое снижение уровня своей зависимости от американских и китайских компаний и технологий в IT-сфере. Иными словами, «цифровой суверенитет» имеет не только военно-политическое или ценностно-культурное измерение, но и экономическое измерение в виде расширения стимулов инвестировать в

---

[72] Aaronson S. A. The digital trade imbalance and its implications for internet governance // Centre for International Governance Innovation: Working Paper №25/2016. 40 p.

[73] Ferracane M. Restrictions on Cross-Border Data Flows: A Taxonomy // European Centre for International Political Economy: Working Paper №1/2017. 27 p.

развитие собственных IT-компаний, которые в будущем выступят фактором роста.

Доминирование концепций секьюритизации в дискурсе об информационной безопасности и регулировании цифрового пространства вызывает опасения, поскольку чрезмерная озабоченность государств вопросами «цифрового суверенитета» может привести к фрагментации Интернета, превратив глобальную сеть в разрозненную совокупность национальных сегментов. Подобные шаги расцениваются как негативные с точки зрения экономического роста, социального и культурного прогресса[74]. Аксиология интернет-пространства не предполагает его избыточной регуляции, тем более на уровне отдельных государств, что чревато рисками «цифровой изоляции».

Наднациональные объединения региональной экономической интеграции, в которых формируется как единый внутренний рынок, так и единые стандарты/нормы его регулирования, также заинтересованы в том, чтобы цифровое пространство входящих в него государств тоже было интегрировано, подчинено единым правилам. В этой связи можно говорить о «цифровом суверенитете» не только государств, но и, например, Европейского союза, для которого крайне важно не проиграть конкурентную борьбу в секторе информационных технологий[75].

Концептуализация понятия «суверенитет» применительно к наднациональным объединениям — это еще одна дискуссионная сфера, поскольку традиционные подходы основываются на том, что носителем суверенитета как верховной власти на определенной территории может быть исключительно государство. Однако в настоящее время происходит серьезная трансформация классических подходов, и основными триггерами здесь выступают два процесса — глобализация и информатизация. В ходе

---

[74] Mueller M. Will the internet fragment? Sovereignty, globalization and cyberspace. Polity, 2017. P. 53.

[75] См. например: Зиновьева Е., Булва В. Цифровой суверенитет ЕС // Современная Европа. 2021. №2. С. 40-49.

регионализации суверенитет размывается и передается на наднациональный и субнациональный уровни публичного управления, а вследствие информатизации суверенитет преломляется через призму виртуальной реальности, которая начинает существовать параллельно физической реальности.

Примерно со второй половины XX века можно наблюдать тенденцию к снижению самостоятельности национальных государств и к делегированию части суверенных полномочий на наднациональный уровень (особенно в рамках процессов региональной экономической интеграции, где подразумевается создание наднациональных институтов, чьи решения имеют приоритет перед нормами национального правопорядка).

Объяснение этим процессам в международных отношениях сначала было дано в рамках неореализма, который не претендовал на кардинальный пересмотр классических концепций суверенитета и не отрицал, что их первичным носителем выступает государство. При этом сам характер взаимодействия между государствами на международной арене стал приобретать форму не прямого столкновения национальных суверенитетов (как в первой половине XX в.), а своеобразной «паутины» переплетающихся государственных суверенитетов[76].

В подобном контексте глобализация может быть рассмотрена не как угроза для самой концепции государственного суверенитета, а как вызов для форм ее практического воплощения, которые должны быть адекватны современным условиям[77].

Так, в частности, проявление подобного подхода можно заметить еще в трудах М. Хиршлера и Б. Циммермана конца XX в., посвященных анализу западноевропейской интеграции. Как отмечают эти исследователи, создание Европейского объединения угля и стали (ЕОУС) стало основой для

[76] Kennedy P., Messner D. Global Trends and Global Governance. Sterling: Pluto Press, 2002. P. 143-144.
[77] ibid. P. 37-40.

формирования наднациональных институтов, наделенных полномочиями по самостоятельному установлению общеобязательных для всех граждан государств-членов требований и правил поведения. При этом (в отличие от прежних интеграционных объединений) ЕОУС, по мнению исследователей, основывался не на прямом представительстве государств-участников, а на создании посредством представительства обособленных самостоятельных органов управления, которые напрямую не зависят от стран, направивших своих представителей в такие органы. Таким образом, деятельность ЕОУС оказалась сконцентрированной на его собственных интересах, определяемых государствами-членами только косвенно. В то же время, подчеркивали М. Хиршлер и Б. Циммерман, подобная ситуация не повлекла за собой утрату государственного суверенитета странами – членами ЕОУС. Они лишь передали часть своих суверенных полномочий для осуществления на наднациональном уровне[78]. Иными словами, если и можно говорить о некоем «суверенитете» наднациональных организаций, то, по мнению неореалистов, он носит исключительно производный, вторичный характер.

В конце XX в. зародился еще один подход к пониманию суверенитета, базирующийся на более общих идеях постмодернизма и постиндустриализма и получивший название постпозитивизма. Ключевой идеей, лежащей в основе постпозитивистского подхода, является мысль о том, что в эпоху глобализации традиционные представления о государственном (национальном) суверенитете утратили всякий смысл, поскольку само государство начало исчезать[79]. Привычные иерархии, по мнению постпозитивистов, постепенно будут разрушены.

Традиционные суверенные полномочия государств, согласно постпозитивистам, сегодня все больше переходят на другие уровни: на

---

[78] Хиршлер М., Цимерман Б. Западно-европейские интеграционные объединения. Право: пер. с нем. / под общ. ред. и предисл. Э. М. Аметистова, М. И. Брагинского. М., 1987. С. 75-77.

[79] См., например: Agamben G. Homo Sacer. Sovereign Power and Bare Life. Stanford: Stanford University Press, 1998. 217 p.; Филиппов А. Суверенитет // Апология. 2005. № 3. С. 58–67.

уровень частных акторов, в своей деятельности напрямую не контролируемых государством (транснациональные корпорации, международные некоммерческие организации); на уровень внутригосударственных субъектов, муниципалитетов и иных административно-территориальных образований (субнациональный уровень); на уровень международных институтов (транснациональный уровень).

«Глобальные потоки финансов, медийных образов, рисков, образцов потребления, народонаселения и власти лишают устойчивости традиционное понятие национальных пространственных границ»[80], и, следовательно, категорию государственного суверенитета. В частности, по мнению Р. Фалка, являющегося сторонником постпозитивистского подхода, суверенитет в эпоху глобализации более не выступает в качестве ключевого признака национального государства. Одновременно, на смену традиционной суверенной деятельности государств приходит функционирование наднациональных институтов, которые сегодня и наделены полномочиями по регулированию мировых процессов (т.е. обладают суверенитетом)[81].

Более того, в рамках постпозитивизма традиционный государственный суверенитет рассматривается в качестве опасного и вредного явления, которое способствует сохранению условий для произвола со стороны национальных государств. Так, постпозитивисты полагают, что государство часто использует традиционный концепт суверенитета для искусственного помещения значимых для него вопросов в сфере национальной безопасности, что, тем самым, формирует квазилегитимную базу для применения насилия по отношению к инакомыслящим[82].

---

[80] Outhwaite W., Ray L. Social Theory and Postcommunism. Oxford: Balckwell, 2005. P. 123.
[81] Falk R. Sovereignty. The Oxford Companion to Politics of the World. New York, Oxford, 1993. P. 853.
[82] Marchart O. The Other Side of Order: Towards a Political Theory of Terror and Dislocation // Parallax. 2003. Vol. 9. № 1. P. 102-111.

Подобная радикальность постпозитивизма представляется несколько излишней и не соответствующей действительности. На это, в частности, указывают и представители неолиберального подхода к пониманию суверенитета, которые вполне справедливо указывают на то, что тезис о конце национального суверенитета аргументирован достаточно слабо, а сам государственный суверенитет сохраняется и в настоящее время, лишь приспосабливаясь к меняющимся условиям эпохи глобализации[83]. Данная точка зрения является доминирующей и в современной отечественной науке[84]. Именно такой позиции мы и будем придерживаться в настоящей работе.

Тем не менее, несмотря на излишнюю радикальность постпозитивистов, стоит отметить, что в условиях глобализации и формирования наднациональных интеграционных объединений, классические концепции суверенитета должны быть трансформированы таким образом, чтобы учитывать специфику передачи определенных полномочий на уровень наднациональных институтов.

Представляется, что наиболее оптимальным способом подобной трансформации может стать конструкция, предложенная неореалистами, в рамках которой при наделении интеграционных институтов полномочиями в традиционно суверенных сферах государственной деятельности речь должна идти не о делегировании части суверенитета, а о выборе формы реализации своих суверенных полномочий государствами – членами интеграционного объединения. При этом сохранение непосредственно суверенитета именно за государствами обеспечивается возможностями по выходу из состава интеграционного объединения, после чего реализация переданных

---

[83] Sørensen G. Sovereignty: Change and Continuity in a Fundamental Institution // Political Studies. 1999. Vol. XLVII. P. 590–604. P. 590-604.

[84] См., например: Кольцов А.Н. О глобализации и суверенитете государств // Вестник Чувашского университета. 2004. № 1. С. 50-53; Самарин А.А. Право и экстерриториальность в условиях глобализации // Вестник Саратовской государственной юридической академии. 2015. № 1 (102). С. 115-124 и др.

полномочий будет возвращена к своим традиционным национальным формам.

Второй вызов для суверенитета — это цифровизация. Так, идеи о необходимости включения новых технологических аспектов в содержание категории «суверенитет» возникли еще до становления цифрового общества в его актуальном виде. Уже в 1980-х гг. в западных исследованиях получила свое закрепление концепция «технологического суверенитета», в рамках которой были предприняты попытки интеграции в соответствующую сферу суверенного ведения государств в части развития технологий. В частности, П. Грант под технологическим суверенитетом понимал «способность и свободу [государства] выбирать, генерировать или приобретать и применять, строить и эксплуатировать коммерческие технологии, необходимые для промышленных инноваций»[85]. Подобный подход является крайне узким и отражает, скорее, конкретные проблемы, свойственные для американского общества 80-х гг. XX в., однако сама направленность идей исследователя свидетельствует о начале зарождения новых подходов к наполнению суверенитета.

На сегодняшний день исследование особенностей учета цифровых аспектов в категории «суверенитет» является достаточно популярным направлением для анализа как в западной, так и в отечественной специальной литературе. При этом в западной доктрине цифровой суверенитет преимущественно рассматривается в контексте деятельности государства по контролю над информационными потоками[86].

В российских же работах цифровой суверенитет воспринимается несколько шире и предполагает включение в суверенную сферу государств

---

[85] Grant P. Technological sovereignty: forgotten factor in the «hitech» razzamatazz // Prometheus. 1982. Т. 1. № 2. P. 239-270.

[86] См., например: O'Neill B. Broadcast Sovereignty in a Digital Environment. Dublin Institute of Technology, 2006. P. 179-197; Couture S., Toupin S. What does the notion of «sovereignty» mean when referring to the digital? // New Media & Society. 2019. № 21(10). P. 2305-2322.

противодействие любым информационным угрозам[87]. Например, М.М. Кучерявый предлагает рассматривать цифровой суверенитет как верховенство и независимость в рамках разработки и осуществления государственной информационной политики не только вовнутригосударственной информационной сети, но и на полях глобального информационного пространства[88]. В свою очередь, Д.В. Винник полагает, что цифровой суверенитет представляет собой возможность государства самостоятельно определять и устанавливать правовой и политический режимы обращения данных в сети Интернет[89]. Из этих определений очевидно, что речь не идет о некоем новом феномене; авторы лишь указывают, что суверенитет государства должен в полной мере распространяться и на сетевое пространство, которое не может находиться ни «само по себе» (поскольку это попросту невозможно), ни под контролем других государств в силу конкурентной природы международных отношений.

Необходимость подобного расширения содержания государственного суверенитета в настоящее время признается и на уровне ООН. Данный вывод был сделан в Докладе группы правительственных экспертов, подготовленном к 68 сессии Генеральной Ассамблеи ООН. В соответствии с выводами данного доклада было прямо установлено, что государственный суверенитет (а также международные нормы, связанные с ним) в полной мере распространяется и на действия государства в собственном информационном пространстве. Кроме того, к сфере суверенитета был отнесен контроль

---

[87] См., например: Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6(51). С. 76-91.

[88] Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2014. № 9. С. 8-15.

[89] Винник Д.В. Цифровой суверенитет: политические и правовые режимы фильтрации данных // Философия науки. 2014. № 2 (61). С. 95-113.

государства над информационно-коммуникационной инфраструктурой, расположенной на их территории[90].

Суммируя приведенные выше определения цифрового суверенитета, можно сделать вывод о том, что под ним следует понимать верховенство государств в отношении собственных информационных пространств и возможность самостоятельно (в отсутствие внешнего вмешательства любых третьих лиц) определять правовой режим создания и распространения информации, правила ведения деятельности в информационных пространствах, требования в сфере безопасности информационных пространств, а также правовой режим создания и функционирования инфраструктуры информационных пространств и иные вопросы, связанные с реализацией государственного суверенитета в собственном информационном пространстве.

Отметим, что развитие представлений о цифровом суверенитете привело к актуализации дискуссии о соотношении государственного суверенитета и передачи государственных полномочий на наднациональный уровень. Иными словами, возникла насущная необходимость совместить доктринальные представления о том, как трансформировалось понимание суверенитета под влиянием глобализации и информатизации. Поскольку «цифровой суверенитет» был признан за государствами, стали возникать вопросы о возможности передачи соответствующих полномочий на наднациональный уровень.

В частности, о возможности формирования наднационального цифрового суверенитета в настоящее время активно говорится на уровне ЕС[91], где предполагается обеспечить вестфальский суверенитет в цифровом пространстве не на уровне отдельных государств – членов ЕС, а на уровне

---

[90] Зиновьева Е.С. Проблемы международного управления Интернетом в контексте цифрового суверенитета // Международная жизнь. 2020. Специальный выпуск. С. 133-137.

[91] Kelly E. Decoding Europe’s new fascination with «tech sovereignty» // Science/Business. 2020. № 9. [Электронный ресурс]. Режим доступа: https://sciencebusiness.net/news/decoding-europes-new-fascination-tech-sovereignty (дата обращения: 07.11.2024).

интеграционного объединения в целом[92]. Ключевым предлогом для реализации цифрового суверенитета сразу на уровне ЕС выступает тезис о том, что у отдельных стран – членов ЕС недостаточно сил для противодействия современным негативным тенденциям в цифровой сфере и для защиты собственных национальных интересов в ней. Не менее значимо и уже отмечавшееся ключевое свойство интеграционных проектов — наличие внутреннего рынка, подчиненного единым правовым нормам. Невозможно обеспечить общие стандарты для оборота благ в физической реальности, проигнорировав аналогичные процессы в сетевом пространстве.

Можно констатировать, что на сегодняшний день цифровой суверенитет ЕС находится только в стадии формирования и представляет собой всего лишь амбициозный проект. Во многом от форм его развития будет зависеть необходимость коренной трансформации категории «суверенитет» в целом. В случае создания цифрового суверенитета ЕС таким образом, что на наднациональном уровне окажутся сформированы полномочия, недоступные для отдельных государств – членов ЕС, можно будет говорить о передаче на уровень интеграции именно части суверенитета стран-участниц (а точнее — о создании нового вида суверенитета, доступного только на наднациональном уровне). В случае же, если на уровень ЕС будут переданы традиционные полномочия государств-членов в информационной сфере, то можно будет придерживаться традиционных неореалистических подходов к соотношению государственного суверенитета и наднациональности.

§ 1.3. Основные направления наднационального регулирования общественных отношений в цифровой сфере

Вызовы современной цифровой эпохи порождают потребность в формировании специфического регулирования не только на национальном,

[92] Зиновьева Е., Булва В. Указ. соч. С. 48.

но и на наднациональном уровне. Круг вызовов для наднационального регулирования, связанных с широкомасштабной цифровизацией общественной жизни, настолько широк, что сегодня все чаще решение соответствующих проблем обеспечивается не по отдельности, а комплексно — в рамках правового регулирования цифрового пространства в целом. Однако подобное комплексное регулирование представляет собой совокупность ряда направлений, находящихся в тесной связи друг с другом, но, тем не менее, обладающих собственными отличительными характеристиками в рамках системы наднационального регулирования цифрового пространства.

В наиболее общем виде к составным элементам наднационального регулирования цифрового пространства можно отнести следующие ключевые направления[93]:

1) наднациональное регулирование порядка обращения персональных данных в рамках единого цифрового пространства;

2) наднациональное регулирование порядка доступа к официальной государственной информации и иным неперсональным данным в пространстве интеграционного объединения;

3) наднациональные правила в сфере защиты интеллектуальной собственности и авторских прав в рамках единого цифрового пространства интеграционного объединения;

4) наднациональное регулирование единого цифрового рынка и порядка предоставления цифровых услуг;

5) наднациональные правила в сфере защиты конкуренции и запрета дискриминации по признаку страны происхождения на единых рынках цифровых услуг;

---

[93] Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. 2023. № 1. С. 12–25.

6) наднациональное регулирование цифровых публичных закупок, осуществляемых на едином рынке интеграционного объединения;

7) наднациональные требования к надежности, безопасности, устойчивости (прежде всего, экологической) и защищенности информационно-коммуникационной инфраструктуры;

8) наднациональные основы совместного противодействия киберпреступности и кибертерроризму, а также обеспечения кибербезопасности.

Как можно заметить, перечень направлений наднационального регулирования общественных отношений в цифровой сфере весьма разнообразен, что обусловлено ее ролью и значением в современной общественной жизни.

Наиболее явно отмеченная особенность сегодня проявляется на уровне наднационального регулирования общественных отношений в цифровой сфере, которое сегодня существует (и разрабатывается) в рамках Европейского союза. Так, ЕС предпринимаются попытки сформировать комплексное наднациональное регулирование, которое бы полностью охватывало все отмеченные выше сферы[94].

1. Наднациональное регулирование порядка обращения персональных данных в рамках единого цифрового пространства на уровне ЕС сегодня регулируется Общим регламентом о защите персональных данных[95], в соответствии с которым установлены коммунитарные правила, обеспечивающие формирование унифицированного режима сбора, хранения и использования персональных данных на всей территории Европейского союза. Кроме того, данным регламентом также закрепляются правовой режим трансграничной передачи персональных данных и выводы

[94] Лю К.А. Указ. соч. С. 15.

[95] 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) // OJ L 119, 4.5.2016, p. 1–88.

персональных данных за пределы цифрового пространства ЕС. Также в Регламенте находят свое отражение право пользователей сети Интернет на псевдоним, право на забвение в сети Интернет. Регламентом устанавливается и наличие специальных должностных лиц, уполномоченных обеспечивать защиту персональных данных[96].

2. Наднациональное регулирование порядка доступа к официальной государственной информации и иным неперсональным данным в пространстве интеграционного объединения также присутствует в рамках ЕС.

Соответствующие коммунитарные правила были закреплены в рамках Регламента о свободном обращении неперсональных данных на территории ЕС[97]. Данным регламентом, в частности, устанавливаются наднациональные требования к хранению и обработке неперсональных данных, особенности хранения данных в облачной инфраструктуре, порядок доступа к данным со стороны органов государственной власти, правила ведения электронного документооборота и особенности обращения неперсональных данных в цифровом пространстве.

В настоящее время развитие наднационального регулирования порядка доступа к официальной государственной информации и иным неперсональным данным в пространстве интеграционного объединения осуществляется на основании Европейской стратегии данных[98].

3. Наднациональные правила в сфере защиты интеллектуальной собственности и авторских прав в цифровом пространстве также

---

[96] Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Сибирское юридическое обозрение. 2019. №1. С. 29-35.

[97] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union // OJ L 303, 28.11.2018, p. 59–68.

[98] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A European strategy for data (COM/2020/66 final). Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (accessed: 30.05.2022).

представлены в качестве самостоятельного направления наднационального регулирования в правопорядке ЕС.

Европейской комиссией еще в 2011 г. было инициировано подписание Меморандумов о взаимопонимании между правообладателями и лицами, косвенно способствующими распространению контрафактной продукции через сеть Интернет или создающим источники доходов для размещения цифровых продуктов в сети Интернет без согласия их правообладателей. Подобными лицами, в частности, являются рекламодатели, которые соглашаются размещать объявления на сайтах с «пиратским» контентом, интернет-магазины, онлайн-медиа и грузоперевозчики, которые способствуют реализации контрафактной продукции и иные «заинтересованные лица» (в терминах Еврокомиссии). При этом подобные меморандумы предполагают привлечение к подписанию «заинтересованных сторон» не только из ЕС, но и из третьих стран[99].

Наиболее актуальным примером подобных меморандумов является Меморандум о взаимопонимании в сфере интернет-рекламы и правах на интеллектуальную собственность 2018 г.[100] Данный меморандум был подписан по итогам собрания всех потенциально заинтересованных сторон, включая представителей рекламной индустрии, онлайн-посредников, представителей сектора по защите контента в сети Интернет, онлайн-медиа, правообладателей, представителей гражданского общества, организаций-потребителей и рекламодателей. Стороны пришли к соглашению о необходимости ограничения доходов «пиратов» от размещения рекламы на сайтах, которые нарушают права интеллектуальной собственности.

Однако отмеченный шаг стал лишь первым этапом в формировании наднационального подхода ЕС к защите интеллектуальной собственности в сети Интернет. Серьезный прорыв в сфере противодействия нарушениям

---

[99] Лю К.А. Указ. соч. С. 20.

[100] Memorandum of understanding on online advertising and intellectual property rights (21.06.2018) [Electronic source] // European Commission. URL: https://ec.europa.eu/docsroom/documents/30226 (accessed: 30.05.2022).

авторских прав в сети Интернет был осуществлен с принятием Регламента о цифровых услугах (DSA)[101] и Регламента о цифровых рынках (DMA)[102], в которых нашло свое отражение комплексное регулирование порядка защиты интеллектуальной собственности в сети Интернет. В частности, в Регламенте о цифровых услугах закреплено понятие незаконного контента, а на лиц, предоставляющих посреднические цифровые услуги (веб-сайты, онлайн-видеохостинги, стриминговые платформы и т.д.), возложена обязанность удалять незаконный контент на основании распоряжений уполномоченных административных или судебных органов государств – членов ЕС.

4. Наднациональное регулирование единого цифрового рынка и порядка предоставления цифровых услуг, впрочем, представляет собой ключевую цель принятия Регламента о цифровых услугах и Регламента о цифровых рынках. Они включают в себя (помимо мер дополнительной защиты интеллектуальной собственности в сети Интернет) целую систему наднационального регулирования цифрового рынка ЕС. Принятие данных регламентов обеспечило формирование актуального режима функционирования единого цифрового рынка с наиболее полной реализацией принципов свободы движения товаров и услуг в ЕС.

При этом в части организации свободного движения цифровых услуг и регулирования особенностей их предоставления на едином рынке ЕС ключевую роль играет Регламент о цифровых услугах. Под действие данного регламента попадают веб-сайты, онлайн-хостинги, онлайн-платформы хранения данных, а также любые иные лица, которые оказывают «посреднические» услуги по передаче, хранению, распределению или размещению информации в сети Интернет.

---

[101] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) PE/30/2022/REV/1 // OJ L 277, 27.10.2022, p. 1–102.

[102] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) PE/17/2022/REV/1 // OJ L 265, 12.10.2022, p. 1–66.

Отличительной особенностью Регламента о цифровых услугах является экстерриториальный характер его действия. Обязанность его соблюдения распространяется на любых лиц (вне зависимости от места их нахождения, резидентства или инкорпорации), оказывающих цифровые услуги физическим и юридическим лицам, являющихся резидентами ЕС.

5. Одновременно Регламент о цифровых услугах и Регламент о цифровых рынках содержат в себе новые антимонопольные правила, подлежащие применению непосредственно в сети Интернет и распространяющиеся на особых субъектов, занимающих доминирующее положение именно в цифровом пространстве (*gatekeepers*).

В рамках данного направления наднационального регулирования общественных отношений в цифровой среде ключевую роль играет Регламент о цифровых рынках[103]. Основной целью принятия данного регламента выступает формирование новой правовой категории — цифровых привратников (англ. *gatekeepers*). Это IT-компании, которые осуществляют поставку цифровых услуг в качестве базовой цифровой платформы: информационно-посреднических услуг в сети Интернет; поисковых услуг; услуг по созданию и поддержанию функционирования социальных сетей; услуг по обмену видео; услуг в сфере обеспечения межличностной коммуникации; услуг по созданию и обслуживанию операционных систем; услуг в сфере облачных вычислений. При этом под соответствующее регулирование также попадает деятельность компаний-привратников по предоставлению рекламных услуг на принадлежащих им цифровых платформах.

Регламент о цифровых рынках формирует особый правовой режим функционирования подобных компаний, возлагает на них серьезные дополнительные обязанности и ограничения. При этом регулирование деятельности цифровых привратников планируется осуществлять по

[103] Лю К.А. Указ. соч. С. 22.

аналогии с регулированием деятельности субъектов естественных монополий. Таким образом, Регламент о цифровых рынках представляет собой не просто правовой механизм наднационального регулирования цифровой сферы, но весьма прогрессивный шаг для права в целом, которое по состоянию на текущий момент не отличается высокой проработанностью в сфере регулирования деятельности цифровых монополий и олигополий[104].

При этом Регламент о цифровых рынках (как и Регламент о цифровых услугах) планируется наделить экстерриториальным действием, распространив его требования на любые компании-привратники, которые предоставляют или предлагают свои услуги конечным пользователям, зарегистрированным или проживающим на территории ЕС.

6. Наднациональное регулирование цифровых публичных закупок, осуществляемых на едином рынке интеграционного объединения, также активно развивается. Данное направление наднационального регулирования включает в себя два не связанных друг с другом аспекта: во-первых, здесь ведется работа по расширению практики использования цифровых сервисов для проведения публичных закупок (*digital procurement*); во-вторых, формируются наднациональные правила и стратегии осуществления публичных закупок инновационных товаров и услуг (*innovation procurement*)[105].

В рамках первого субнаправления в ЕС приняты такие акты, как Сообщение Комиссии о сквозных электронных закупках[106]; Директива об электронном выставлении счетов-фактур в сфере публичных закупок[107]; Исполнительный регламент Комиссии о формах публикации уведомлений о

---

[104] Лю К.А. Указ. соч. С. 22.
[105] Там же. С. 23.
[106] Communication from the Commission to the European parliament, the Council, the European economic and social committee and the Committee of the regions «End-to-end e-procurement to modernize public administration» (COM/2013/0453 final) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0453 (accessed: 30.05.2022).
[107] Directive 2014/55/EU of the European Parliament and of the Council of 16 April 2014 on electronic invoicing in public procurement // OJ L 133, 6.5.2014, p. 1–11.

госзакупках[108], а также отдельные положения общей Директивы о государственных закупках[109] и др. Данные акты ориентируют государства – члены ЕС на расширение практики использования цифровых технологий при проведении публичных закупок, формируют единые электронные формы документов, процедуры осуществления закупок в электронной форме и т.д.

В свою очередь, второе субнаправление наднационального регулирования цифровых закупок предполагает создание общей коммунитарной основы для осуществления публичных закупок в сферах цифровой и облачной инфраструктуры[110]. Правовой основой тут выступают положения Директивы о государственных закупках, касающиеся особенностей осуществления закупочной деятельности в инновационных сферах. Кроме того, в данной сфере также планируется формирование единой коммунитарной системы публичных закупок, осуществляемых в целях создания, развития и поддержания функционирования цифровой и облачной инфраструктуры[111]. При этом осуществление подобных закупок тесно связывается с необходимостью совершенствования наднационального регулирования в сфере обеспечения безопасности подобной инфраструктуры[112].

7. Таким образом, предыдущее направление наднационального регулирования общественных отношений в цифровой сфере оказывается тесно связано с коммунитарным регулированием для обеспечения развития,

---

[108] Commission Implementing Regulation (EU) 2015/1986 of 11 November 2015 establishing standard forms for the publication of notices in the field of public procurement and repealing Implementing Regulation (EU) No 842/2011 // OJ L 296, 12.11.2015, p. 1–146.
[109] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC // OJ L 94, 28.3.2014, p. 65–242.
[110] Лю К.А. Указ. соч. С. 23.
[111] Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper). European Court of Auditors. 2019. 74 p.
[112] Madiega T. Digital sovereignty for Europe. European Parliamentary Research Service (EPRS) Ideas Paper. July 2020. 12 p.

надежности, безопасности, устойчивости[113] (прежде всего, экологической) и защищенности информационно-коммуникационной инфраструктуры.

Формирование безопасной, высокопроизводительной и устойчивой цифровой инфраструктуры представляет собой одну из ключевых задач, стоящих перед наднациональным регулированием ЕС на текущем этапе[114].

Основы соответствующего регулирования были заложены в переработанном Европейском кодексе электронных коммуникаций[115], которым были установлены ключевые требования к созданию, функционированию и защите информационно-коммуникационной инфраструктуры в масштабах всего Европейского союза. Вопросам обеспечения безопасности информационно-коммуникационной инфраструктуры посвящены положения Директивы об обеспечении общего высокого уровня кибербезопасности в Союзе[116] (Директива NIS 2).

Вместе с тем в рамках анализируемого направления наднационального регулирования сегодня складывается новое регулирование, связанное уже не с ИКТ-инфраструктурой, а с облачной. Создание облачной инфраструктуры планируется обеспечить за счет активизации инновационных закупок, совершенствования коммунитарного регулирования порядка обращения неперсональных данных, введения в действие Регламентов о цифровых рынках и о цифровых услугах, создания наднациональной правовой базы для

---

[113] Речь здесь идет о реализации концепции устойчивого развития, предполагающей гармоничное развитие бизнеса, общества и окружающей среды (см., например, Резолюция Генеральной Ассамблеи ООН от 25 сентября 2015 года A/RES/70/1 «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года» // [Электронный ресурс] // Режим доступа: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=R (дата обращения: 30.05.2022)).

[114] Лю К.А. Указ. соч. С. 23.

[115] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (PE/52/2018/REV/1) // OJ L 321, 17.12.2018, p. 36–214.

[116] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (PE/32/2022/REV/2) // OJ L 333, 27.12.2022, p. 80–152.

развития облачных вычислений. Основой для реализации соответствующей деятельности выступает Европейская стратегия данных[117].

При этом особое внимание в рамках всего исследуемого направления уделяется вопросам обеспечения энерегоэффективности и экологической нейтральности[118] создаваемой и уже функционирующей цифровой и информационно-коммуникационной инфраструктуры в соответствии с принципами Европейской зеленой сделки[119]. Формирование соответствующего регулятивного механизма было возложено на Еврокомиссию, которая должна разработать и утвердить расширенные индексы цифровой экономики и общества (англ. Digital Economy and Society Index, DESI[120]).

8. Наднациональные основы совместного противодействия киберпреступности и кибертерроризму, а также обеспечения кибербезопасности.

В рамках данного направления наднационального регулирования на уровне ЕС еще в 2013 г. была принята Стратегия кибербезопасности ЕС[121]. В

---

[117] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A European strategy for data (COM/2020/66 final). Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (accessed: 30.05.2022).

[118] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 30.05.2022).

[119] Communication from the Commission to the European Parliament, the European council, the Council, the European economic and social committee and the Committee of the regions: The European Green Deal (COM/2019/640 final). Brussels, 11.12.2019 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN (accessed: 30.05.2022).

[120] The Digital Economy and Society Index [Electronic source] // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 30.05.2022).

[121] Joint communication to the European Parliament, the Council, the European economic and Social Committee and the Committee of the regions «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace» (JOIN (2013) 1 final). Brussels, 7.2.2013 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 (accessed: 30.05.2022).

2016 г. требования к обеспечению кибербезопасности нашли свое отражение в рамках Директивы по безопасности сети и информационных систем[122] (Директива NIS). В 2017 г. Комиссия выпустила Рекомендацию в сфере общего уровня безопасности сетей и информационных систем в ЕС[123]. Особый всплеск законотворческой активности пришелся на 2018-2019 гг., когда был принят целый набор законодательных актов в сфере кибербезопасности[124], включающий в себя, в том чисел, Регламент о кибербезопасности[125]. Наконец, в 2022 г. была принята новая Директива об обеспечении общего высокого уровня кибербезопасности в Союзе[126] (Директива NIS 2), в которой были закреплены актуальные наднациональные основы обеспечения кибербезопасности в ЕС[127].

Также обеспечение кибербезопасности осуществляется на основе Регламента о защите персональных данных. Он призван обеспечить надежное хранение и обработку таких данных с максимальным снижением рисков несанкционированного доступа. Предполагается установление новых требований к кибербезопасности в сфере публичных закупок.

С 2005 г. на уровне ЕС действует Агентство Европейского союза по кибербезопасности (European Union Agency for Cybersecurity). Регламент о

---

[122] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // OJ L 194, 19.7.2016, p. 1–30.

[123] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises // OJ L 239, 19.9.2017, p. 36–58.

[124] Joint Communication to the European Parliament and the Council «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU» (JOIN/2017/0450 final) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (accessed: 30.05.2022).

[125] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // OJ L 151, 7.6.2019, p. 15–69.

[126] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (PE/32/2022/REV/2) // OJ L 333, 27.12.2022, p. 80–152.

[127] Касьянов Р. А. Международный опыт противодействия киберугрозам // Российский следователь. 2023. № 6. С. 59-63.

кибербезопасности существенно расширил полномочия данного агентства и наделил его дополнительными ресурсами. Кроме того, для обеспечения кибербезопасности на уровне ЕС было создано Объединенное подразделение по кибербезопасности (*англ. Joint Cybersecurity Unit*)[128], которое обеспечивает более тесную координацию между наднациональными институтами ЕС и органами государственной власти государств – членов ЕС.

Таким образом, на уровне ЕС в настоящее время сложилось наднациональное регулирование по всем выявленным направлениям.

На уровне ЕАЭС сегодня также ведется деятельность по формированию наднациональных правовых основ для регулирования цифровых общественных отношений. Однако круг вопросов, подлежащих наднациональному регулированию, на данный момент значительно уже[129].

Соответствующие положения можно встретить в рамках дополнительных протоколов к Договору о Евразийском экономическом союзе[130] (в частности, в Протоколе об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза[131], которым устанавливаются общие особенности обмена неперсональными государственными данными в рамках ЕАЭС). Некоторой гармонизации также подвергается регулирование осуществления государственных закупок в электронной форме. Кроме того, в настоящее

---

[128] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (PE/28/2021/INIT) // OJ L 202, 8.6.2021, p. 1–31.

[129] Лю К.А. Указ. соч. С. 24.

[130] Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014) // Официальный сайт Евразийской экономической комиссии http://www.eurasiancommission.org/, 05.06.2014.

[131] Приложение № 3 к Договору о Евразийском экономическом союзе. Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза [Электронный ресурс] // Режим доступа: https://docs.eaeunion.org/ru-ru/Pages/DisplayDocument.aspx?s=bef9c798-3978-42f3-9ef2-d0fb3d53b75f&w=632c7868-4ee2-4b21-bc64-1995328e6ef3&l=540294ae-c3c9-4511-9bf8-aaf5d6e0d169&EntityID=3610 (дата обращения: 30.05.2022).

время в ЕАЭС реализуется Цифровая повестка, принятая в 2016 г.[132], которая предполагает формирование: 1) цифрового измерения интеграции (электронный документооборот, наднациональные базы данных, межгосударственные цифровые сервисы и услуги); 2) цифровых рынков ЕАЭС; 3) цифровых инфраструктур и цифровых активов ЕАЭС[133].

Однако отмеченные наднациональные акты ЕАЭС не содержат в себе норм, направленных на непосредственное правовое регулирование цифрового пространства на наднациональном уровне. Протоколы представляют собой инструмент гармонизации национальных законодательств в отдельных сферах, а Цифровая повестка ЕАЭС является лишь общим документом стратегического планирования, который содержит максимально широкие политические планы в цифровой сфере[134].

Таким образом, опора на опыт ЕАЭС с меньшей степенью достоверности позволяет установить универсальные направления наднационального регулирования общественных отношений в цифровой сфере.

Тем не менее, если говорить об определении общих направлений интеграционного регулирования цифрового пространства в целом, то нельзя опираться сугубо на опыт ЕС в соответствующей сфере (как минимум, в связи с тем, что направления наднационального регулирования цифрового пространства постоянно расширяются).

В подобных условиях представляется целесообразным выработать универсальный подход к категоризации основных составляющих

---

[132] Заявление о цифровой повестке ЕАЭС [Электронный ресурс] // Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Pages/docs.aspx (дата обращения: 30.05.2022).

[133] Общие подходы к формированию цифрового пространства Евразийского экономического союза в перспективе до 2030 года (Подготовлено ЕЭК в рамках выработки предложений по формированию цифрового пространства ЕАЭС) [Электронный ресурс] // Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Pages/docs.aspx (дата обращения: 30.05.2022).

[134] Лю К.А. Указ. соч. С. 22

интеграционного регулирования единого цифрового пространства. При этом в качестве критерия для подобной категоризации можно использовать предмет регулирования.

По данному критерию все проанализированные выше составляющие интеграционного регулирования цифрового пространства могут быть распределены по трем основным направлениям:

1. наднациональное регулирование порядка обращения данных в цифровом пространстве (интеграционная информационно-коммуникационная политика). Соответствующее направление будет включать в себя обращение персональных данных, обращение неперсональных данных, обмен официальной государственной информацией (в т.ч. в таможенной сфере и в сфере технической стандартизации), создание наднациональных баз данных, создание единых цифровых форм осуществления публичных закупок и иные аналогичные направления, связанные с цифровизацией порядка сбора, анализа, изменения, хранения и обращения любых данных;

2. наднациональное регулирование единых (общих) цифровых рынков (интеграционная политика в сфере цифровых рынков). Данное направление будет включать в себя регулирование цифровых услуг, конкуренции на цифровых рынках, деятельности цифровых компаний, искусственного интеллекта, криптоактивов, цифровых финансов, а также защиту интеллектуальной собственности и авторских прав в цифровом пространстве. В целом к соответствующему направлению могут быть отнесены любые интеграционные акты, регулирующие любые единые (общие) цифровые рынки;

3. наднациональное регулирование цифровой безопасности (интеграционная политика цифровой безопасности), включающее в себя противодействие киберпреступности и кибертерроризму, обеспечение безопасности и защищенности цифровой инфраструктуры, экологическую

безопасность цифровой инфраструктуры, устойчивость цифровой инфраструктуры и иные сферы интеграционного регулирования, связанные с обеспечением надежного, бесперебойного и устойчивого функционирования цифровой инфраструктуры и существования цифровой среды.

Приведенные три направления охватывают собой все сферы интеграционного регулирования цифрового пространства на современном этапе. Именно по данным направлениям должно развиваться интеграционное регулирование цифрового пространства в ЕАЭС.

Глава II. Наднациональное регулирование цифрового пространства в рамках ЕС

§ 2.1. Развитие наднационального регулирования цифрового пространства в ЕС

Осознание необходимости построения единого цифрового пространства, которое может обеспечить как системную цифровую трансформацию входящих в ЕС социально-экономических систем, так и цифровой суверенитет всего Союза, произошло около десяти лет назад. В 2010 г. Еврокомиссия подготовила сообщение «Цифровая повестка дня для Европы»[135]. В ней указывалось на две стратегические цели, находящиеся в тесной взаимосвязи, — построение цифровой экономики и развитие информационного общества. В наиболее общем виде, данные цели формулировались как «обеспечение устойчивых экономических и социальных выгод от единого цифрового рынка», основой которого должен был стать сверхскоростной Интернет.

При этом цели и мероприятия, предусмотренные Цифровой повесткой дня для Европы, составляли одну из семи «флагманских инициатив» более широкого проекта — Стратегии «Европа-2020»[136]. Здесь особо указывалось на социальные выгоды цифровизации: улучшение здравоохранения, более безопасные и эффективные решения в области транспорта, новые возможности для СМИ, упрощенный доступ к социальным услугам и культурно-образовательному контенту. Следует отметить, что в Стратегии подчеркивалось: ЕС пока не контролирует значительную часть принципиально важных информационно-коммуникационных технологий, а

---

[135] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. COM(2010)245 final. Brussels, 19.5.2010. [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R%2801%29 (accessed: 19.12.2022).

[136] Europe 2020. A European strategy for smart, sustainable and inclusive growth [Electronic source]. URL: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf (accessed: 19.12.2022)

главное, не имеет надлежащей правовой основы, в рамках которой можно было бы эффективно осуществлять нужные прорывные решения в цифровой сфере.

В целях преодоления данных рисков в 2011 г. ЕС, прежде всего, обратился к традиционной для соответствующей сферы теме защиты авторских прав в сети Интернет.

Так, Европейской комиссией в 2011 г. было инициировано подписание Меморандумов о взаимопонимании между правообладателями и лицами, косвенно способствующими распространению контрафактной продукции через сеть Интернет или обеспечивающими источники доходов для размещения цифровых продуктов в сети Интернет без согласия их правообладателей. Подобными лицами, в частности, являются рекламодатели, которые соглашаются размещать объявления на сайтах с «пиратским» контентом, интернет-магазины, онлайн-медиа и грузоперевозчики, которые способствуют реализации контрафактной продукции и иные «заинтересованные лица» (в терминах Еврокомиссии). При этом подобные меморандумы предполагают привлечение к подписанию «заинтересованных сторон» не только из ЕС, но и из третьих стран.

Наиболее актуальным примером подобных меморандумов является Меморандум о взаимопонимании в сфере интернет-рекламы и правах на интеллектуальную собственность 2018 г.[137] Данный меморандум был подписан по итогам собрания всех потенциально заинтересованных сторон, включая представителей рекламной индустрии, онлайн-посредников, представителей сектора по защите контента в сети Интернет, онлайн-медиа, правообладателей, представителей гражданского общества, организаций-потребителей и рекламодателей. Стороны пришли к соглашению о

[137] Memorandum of understanding on online advertising and intellectual property rights (21.06.2018) [Electronic source] // European Commission. URL: https://ec.europa.eu/docsroom/documents/30226 (accessed: 19.12.2022).

необходимости ограничения доходов «пиратов» от размещения рекламы на сайтах, которые нарушают права интеллектуальной собственности.

Кроме того, в 2013–2014 гг. на уровне ЕС начинает вестись активная правотворческая работа, направленная на расширение практики использования цифровых сервисов для проведения публичных закупок (*digital procurement*). В рамках данного направления в ЕС были приняты такие акты, как Сообщение Комиссии о сквозных электронных закупках[138]; Директива об электронном выставлении счетов-фактур в сфере публичных закупок[139]; Исполнительный регламент Комиссии о формах публикации уведомлений о госзакупках[140], а также отдельные положения общей Директивы о государственных закупках[141] и др. Данные акты были направлены на расширение практики использования цифровых технологий при проведении публичных закупок, формирование единых электронных форм документов, процедуры осуществления закупок в электронной форме и т.д.

Тем не менее, несмотря на предпринятые шаги, наднациональное регулирование цифрового пространства все еще носило крайне фрагментарный характер и не затрагивало большого количества сфер цифровой общественной жизни, имеющих принципиальное значение для развития европейской интеграции (в частности, речь здесь идет об отсутствии наднационального регулирования цифровых рынков и цифровых услуг).

---

[138] Communication from the Commission to the European parliament, the Council, the European economic and social committee and the Committee of the regions «End-to-end e-procurement to modernize public administration». COM/2013/0453 final.[Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0453 (accessed: 19.12.2022).

[139] Directive 2014/55/EU of the European Parliament and of the Council of 16 April 2014 on electronic invoicing in public procurement // OJ L 133, 6.5.2014, p. 1–11.

[140] Commission Implementing Regulation (EU) 2015/1986 of 11 November 2015 establishing standard forms for the publication of notices in the field of public procurement and repealing Implementing Regulation (EU) No 842/2011 // OJ L 296, 12.11.2015, p. 1–146.

[141] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC // OJ L 94, 28.3.2014, p. 65–242.

На недостаток соответствующего правового регулирования на наднациональном уровне ЕС было указано в 2014 г., когда Еврокомиссией был выпущен разъяснительный документ «Европейский цифровой план»[142], в котором закреплялись цели построения единого цифрового пространства в рамках Союза. Здесь говорилось о том, что цифровой сектор развивается в семь раз быстрее, чем реальная экономика, однако это развитие тормозится отсутствием общеевропейских регуляторных правил и недостаточной координацией между государствами-членами.

Как следствие, новый состав Еврокомиссии 2014 г. под председательством Ж.К. Юнкера объявил построение «единого цифрового рынка» одним из трех приоритетов[143]. С этого момента начался следующий этап развития наднационального регулирования цифрового пространства в ЕС. На данном этапе эволюции наднациональных правовых основ регулирования цифрового пространства в ЕС, учитывая нарастающую информатизацию экономических процессов, ключевую роль в построении цифровой экономики стали играть персональные и неперсональные данные. Именно в этом направлении совершенствования правового регулирования Еврокомиссия под председательством Ж.К. Юнкера сделала существенные шаги.

Так, в 2016 г. был принят один из ключевых европейских актов в области защиты персональных данных — Общий регламент по защите данных[144] (далее также — GDPR). Данным актом было расширено понятие персональных данных, введены понятия «трансграничной передачи данных», псевдонимизации, установлено право на забвение, определен правовой

---

[142] The European Union explained: Digital agenda for Europe [Electronic source]. URL: http://europa.eu/pol/index_en.htm http://europa.eu/!bY34KD (accessed: 19.12.2022).

[143] Сарханянц К. Еврокомиссия стирает границы в онлайне [Электронный ресурс] // URL: http://www.kommersant.ru/doc/2723377 (дата обращения: 19.12.2022).

[144] 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) // OJ L 119, 4.5.2016, p. 1–88.

статус специального должностного лица по защите данных. Основная цель Регламента — полностью унифицировать правила сбора, хранения и обработки персональных данных в ЕС, облегчить правила доступа граждан к данным, которые имеют к ним отношение. Регламент четко распределяет полномочия субъектов обработки персональных данных, распределяет между ними ответственность. Еще одна задача данного акта — унифицировать правила экспорта данных из ЕС, что принципиально важно для внешнеэкономических отношений[145]. GDPR также был направлен на обеспечение кибербезопасности. Он был призван обеспечить надежное хранение и обработку таких данных с максимальным снижением рисков их утечки.

Кроме того, в этом же году были доработаны более общие наднациональные правовые основы регулирования вопросов кибербезопасности посредством принятия специальной Директивы по безопасности сетей и информационных систем 2016 г.[146]. В соответствии с данной директивой предусматривалось повышение уровня безопасности сетей и информационных систем в целях обеспечения надлежащего уровня защиты сервисов и услуг, критически важных для европейского общества и экономики. В частности, Директивой о безопасности сетей и информационных систем предусматривалось формирование в государствах-членах ЕС специальных органов по обеспечению кибербезопасности, создание специальных групп реагирования на угрозы компьютерной безопасности (*англ. Computer-security incident response teams, CSIRT*), а также закреплялись обязательства-государств членов по разработке и принятию национальных стратегий кибербезопасности. Кроме того, в соответствии с

---

[145] Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Сибирское юридическое обозрение. 2019. №1. С. 32.

[146] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // OJ L 194, 19.7.2016, p. 1-30.

Директивой о безопасности сетей и информационных систем были закреплены обязанности поставщиков основных цифровых услуг принимать надлежащие меры кибербезопасности и уведомлять созданные национальные органы о серьезных инцидентах в соответствующей сфере.

В дальнейшем Еврокомиссия под руководством Ж.К. Юнкера продолжила законотворческую работу в сфере формирования эффективной наднациональной правовой базы обеспечения кибербезопасности. Так, в 2017 г. Комиссия выпустила Рекомендацию в сфере общего уровня безопасности сетей и информационных систем в ЕС[147], а в 2018–2019 гг. был принят целый Пакет законодательных актов в сфере кибербезопасности[148], включающий в себя, в том чисел, Регламент о кибербезопасности[149]. Кроме того, в 2018 г. был существенно переработан Европейский кодекс электронных коммуникаций[150], где были установлены ключевые требования к созданию, функционированию и защите информационно-коммуникационной инфраструктуры в масштабах всего Европейского союза.

Параллельно с этими процессами создавались новые подходы в области обеспечения кибербезопасности, новые структуры, уполномоченные решать поставленные вопросы по защите объектов критической инфраструктуры от цифровых угроз. В частности, здесь можно назвать Европейское агентство по сетевой и информационной безопасности (ENISA), Объединенный исследовательский центр (JRC) при Еврокомиссии, Группы

---

147 Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises // OJ L 239, 19.9.2017, p. 36–58.

148 Joint Communication to the European Parliament and the Council «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU» (JOIN/2017/0450 final) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (accessed: 19.12.2022).

149 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // OJ L 151, 7.6.2019, p. 15–69.

150 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (PE/52/2018/REV/1) // OJ L 321, 17.12.2018, p. 36–214.

реагирования на инциденты компьютерной безопасности (CSIRT или CERT), созданные на основе Директивы NIS и т.д.

В 2018 г. также была продолжена работа по совершенствованию наднационального регулирования цифровых данных. В этом году был принят Регламент, создающий правовую основу свободного обращения неперсональных данных на территории ЕС[151]. Цель данного акта — обеспечить свободное обращение и обработку данных, не относящихся к категории персональных, между государственными органами и учреждениями. Эти данные могут храниться и обрабатываться на облачных серверах, расположенных в любом государстве – члене ЕС, и государственные регулирующие органы при необходимости могут получить доступ к ним из любой точки. В рамках данного Регламента также поощряется саморегулирование среди поставщиков облачных сервисов, разработка собственных «кодексов поведения». Эти меры были направлены не только на координацию действий в соответствующей сфере, но и на обеспечение будущей отрасли облачных вычислений.

Таким образом, в рамках данного этапа развития наднационального правового регулирования цифрового пространства в ЕС было обеспечено существенное расширение сфер соответствующего регулирования по сравнению с предыдущим этапом.

С 2020 г. начинается уже ***современный этап*** эволюции наднационального регулирования единого цифрового пространства в ЕС[152]. При этом интенсификация европейской политики в сфере построения единого цифрового пространства первоначально была связана с очередной сменой Председателя Европейской Комиссии, в рамках которой данную

---

[151] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union // OJ L 303, 28.11.2018, p. 59–68.

[152] Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. 2023. № 1. С. 12-25.

должность заняла У. фон дер Ляйен[153]. В 2019 г. она объявила о необходимости достичь цифрового суверенитета ЕС в критических отраслях. Трансформация цифровой политики в соответствии с вызовами цифровой эпохи стала одним из ключевых приоритетов деятельности нового состава Еврокомиссии[154], а ближайший период с 2020 г. по 2030 г. был объявлен Цифровым десятилетием (англ. Digital Decade)[155].

Еще больше необходимость развития наднациональной политики ЕС в цифровой сфере стала очевидной в контексте вызовов глобальной пандемии COVID-19, которые привели к экспоненциальному росту роли и объемов цифровых коммуникаций в 2020–2021 гг. Ограничительные меры, введенные государствами (как в сфере социального дистанцирования, так и в сфере работы бизнеса), повлекли за собой интенсификацию процессов цифровизации во всех сферах общественной жизни[156]. Во время пандемии COVID-19 цифровые технологии стали активно использоваться для работы, обучения, развлечений, общения, доступа к продуктам и услугам, обращения за медицинской помощью (телемедицина) и т.д. Развитие большинства сфер общественной жизни в период пандемии наглядно продемонстрировала огромный трансформационный потенциал цифровых технологий (например, в части удаленной работы, дистанционного обучения, онлайн-доставок продуктов и др.)[157].

---

[153] Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. 2022. № 1. С. 61–75.

[154] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: Shaping Europe's digital future (COM/2020/67 final). Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067 (accessed: 19.12.2022).

[155] A Europe fit for the digital age [Electronic source] // European Commission. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en (accessed: 19.12.2022).

[156] Лю К.А. Указ. соч. С. 63.

[157] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade. COM/2021/118 final. Brussels, 9.3.2021 // [Electronic

Более того, практика более широкого использования цифровых технологий во время пандемии продемонстрировала высокий потенциал их применения для достижения целей Европейской зеленой сделки (*англ. The European Green Deal*)[158]. Освоение цифровых технологий и более активное использование современных ИКТ в бизнесе и государственном управлении было оценено европейскими наднациональными институтами в качестве одного из перспективных путей к климатически нейтральной (с нулевыми выбросами парниковых газов) и устойчивой европейской экономике[159].

Вместе с тем глобальная пандемия COVID-19 выявила наличие серьезных уязвимостей европейского цифрового пространства. В частности, одной из таких сложностей, масштаб которой был осознан в период пандемии, стало наличие серьезной зависимости ЕС от критически важных цифровых решений и технологий, реализуемых зарубежными субъектами на территории ЕС[160]. Обострились проблемы с распространением ложной и вводящей в заблуждение информации в сети Интернет, проблемы в сфере кибербезопасности, а также уязвимости цифровой инфраструктуры ЕС[161].

В подобных условиях Комиссия У. фон дер Ляйен перешла к еще более активным действиям в сфере развития наднационального регулирования

---

source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 19.12.2022).

[158] Communication from the Commission to the European Parliament, the European council, the Council, the European economic and social committee and the Committee of the regions: The European Green Deal. COM/2019/640 final. Brussels, 11.12.2019 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN (accessed: 19.12.2022).

[159] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 19.12.2022).

[160] Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. 2022. № 1. С. 61–75.

[161] Цифровая повестка и инициативы в области цифровых технологий в условиях COVID-19 (обзор практик Европейского союза, Организации экономического сотрудничества и развития, а также других стран). М.: НИУ ВШЭ, 2020. 19 с.

цифрового пространства, отвечающего современным вызовам и угрозам, обострившимся в период пандемии COVID-19.

Так, в сентябре 2020 г. У. фон дер Ляйен в своем послании объявила, что ЕС должен обеспечить укрепление собственного цифрового суверенитета на основе единых целей и принципов, сформулированных в рамках общего видения ЕС[162]. Впоследствии подобное общее видение было подробно сформулировано Европейской комиссией в рамках Цифрового компаса 2030[163], который предполагал интенсификацию цифровой трансформации Европейского союза на основе формирования полностью функционирующего единого цифрового рынка[164].

Необходимость введения новых правил регулирования на цифровых рынках ЕС была обусловлена стремлением наднациональных институтов ЕС (и, прежде всего, Европейской комиссии под председательством У. фон дер Ляйен) предоставить определенные преимущества участникам соответствующих рынков, являющихся резидентами ЕС. Иными словами, на данном этапе эволюции наднационального регулирования цифрового пространства ЕС перешел к *протекционистской политике*, направленной на установление дополнительных требований и барьеров для крупных зарубежных IT-компаний, ведущих свою деятельность на цифровых рынках[165].

---

[162] State of the Union Address by President von der Leyen at the European Parliament Plenary [Electronic source] // European Commission. 16 September 2020 . URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (accessed: 19.12.2022).

[163] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade. COM/2021/118 final. Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 19.12.2022).

[164] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A Digital Single Market Strategy for Europe. COM/2015/0192 final. Brussels, 6.5.2015 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 (accessed: 19.12.2022).

[165] Лю К.А. Указ. соч. С. 70.

В частности, предполагается введение механизма оценки поглощений одних участников высокотехнологичных компаний другими (на основе механизма проверки иностранных инвестиций ЕС[166]). Данная мера направлена на противодействие тренду на приобретение стартапов в цифровой сфере крупными зарубежными IT-гигантами[167]. В рамках данного механизма будет осуществляться проверка соответствия сделок слияния и поглощения требованиям антимонопольного законодательства и законодательства о защите конкуренции. Подобным образом ЕС планирует добиться повышения конкуренции на цифровых рынках, а также обеспечить на них более свободное развитие для предприятий малого и среднего бизнеса.

Кроме того, работа ведется и по направлению трансформации системы налогообложения участников цифровых рынков в сторону создания более благоприятного налогового режима для малого и среднего бизнеса[168]. Несмотря на то, что формально данные изменения налогообложения не будут направлены против зарубежных IT-компаний, по мнению М. Жеро, фактически они все же окажут наиболее отрицательное влияние именно на американских и китайских IT-гигантов, чрезмерное присутствие которых на европейских цифровых рынках рассматривается ЕС в качестве ключевого риска как для развития собственных компаний, так и для обеспечения кибербезопасности и защиты персональных данных пользователей. Таким

[166] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. // OJ L 79I , 21.3.2019, p. 1–14.

[167] Madiega T. Digital sovereignty for Europe. European Parliamentary Research Service (EPRS) Ideas Paper. July 2020. 12 p.

[168] Proposal for a Council directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services. COM/2018/0148 final. Brussels, 21.3.2018 (ongoing) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:148:FIN (accessed: 19.12.2022).

образом, данная мера расценивается в ЕС как один из важнейших шагов на пути к обеспечению цифрового суверенитета[169].

Однако, помимо отмеченных протекционистских мер, построение единого цифрового пространства требовало и наличия более общих регулятивных инструментов, направленных на формирование *наднациональных правил ведения деятельности на цифровом рынке*[170]. Свое отражение они нашли в двух законодательных предложениях Европейской комиссии: в предложении о принятии Регламента о цифровых услугах[171] и в предложении о принятии Регламента о цифровых рынках[172].

Оба «законопроекта» предполагали создание общих нормативных основ регулирования цифровых рынков на наднациональном уровне. В них прямо указывается на создание единого цифрового рынка ЕС. При этом, как отмечалось в самих «законопроектах», они полностью соответствуют существующей нормативной базе ЕС, включая Директиву об электронной торговле 2000 г.[173], Директиву об аудиовизуальных медиасервисах 2010 г.[174], Регламент 2019 г. о продвижении справедливости и прозрачности для бизнес-

---

[169] Gérot M., Maxwell W. Will the GDPR frustrate Europe's plans for AI? [Electronic source] // ItProPortal. March 18, 2020. URL: https://www.itproportal.com/features/will-the-gdpr-frustrate-europes-plans-for-ai/ (accessed: 19.12.2022).

[170] Лю К.А. Указ. соч. С. 71.

[171] Proposal for a Regulation of the European parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. COM/2020/825 final (adopted) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN (accessed: 19.12.2022).

[172] Proposal for a Regulation of the European parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). COM/2020/842 final (adopted) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN (accessed: 19.12.2022).

[173] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) // OJ L 178, 17.7.2000, p. 1-16.

[174] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) // OJ L 95, 15.4.2010, p. 1-24.

пользователей посреднических онлайн-услуг[175] и другим положениям наднационального права ЕС.

По итогам обсуждений в рамках «законодательной» процедуры ЕС предложения Комиссии о принятии регламентов о цифровых услугах и о цифровых рынках были приняты и в сентября–октябре 2022 г. обрели форму Регламента о едином рынке цифровых услуг[176] (*Digital Services Act, DSA*) и Регламента о конкурентных и справедливых рынках в цифровом секторе[177] (*Digital Markets Act, DMA*). Таким образом, начиная с осени 2022 г. на уровне ЕС были окончательно сформированы наднациональные правовые основы для функционирования единого рынка цифровых услуг с особыми антимонопольными требованиями, правилами защиты авторских прав в сети Интернет и иными регуляторными требованиями к функционированию цифрового пространства.

В целом, принятие данных регламентов призвано обеспечить формирование актуального режима функционирования единого цифрового рынка с наиболее полной реализацией принципов свободы движения товаров и услуг в ЕС (подробно положения соответствующих регламентов будут нами проанализированы в параграфе 2.3 настоящего исследования).

Впрочем, сразу же стоит отметить, что компании IT-сектора, на которых были распространены требования DSA и DMA, активно противодействовали его принятию.

В частности, Amazon обратилась в Суд ЕС с требованием снять с нее обязанности по исполнению требований «пилотного» проекта DSA и DMA

---

[175] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services 9 PE/56/2019/REV/1) // OJ L 186, 11.7.2019, p. 57-79.

[176] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) PE/30/2022/REV/1 // OJ L 277, 27.10.2022, p. 1–102.

[177] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) PE/17/2022/REV/1 // OJ L 265, 12.10.2022, p. 1–66.

(еще до вступления данных регламентов в силу). При этом компания указывала на то, что полное исполнение требований «пилотного» режима повлечет за собой причинений ей серьезного и непоправимого ущерба, а также приведет к снижению уровня ее конкурентоспособности по сравнению с другими компаниями цифрового рынка, на которых не распространяются требования «пилотного» проекта DSA и DMA.

Суд ЕС в своих постановлениях[178] по данному делу полностью отклонил доводы Amazon, отметив, что общественный интерес, который защищается DSA и DMA, имеет приоритет перед имущественными и рыночными интересами Amazon. Кроме того, Суд ЕС отметил, что несмотря на непоправимость ущерба, который может быть причинен Amazon, данный ущерб не будет носить серьезного (существенного) характера.

Таким образом, Суд ЕС однозначно встал на сторону европейского законодателя и отметил общую корректность положений DSA и DMA.

Также в части анализа развития наднационального правового регулирования цифрового пространства ЕС после 2020 г. нельзя не отметить выдвинутое Еврокомиссией в 2021 г. Предложение о принятии *Регламента об искусственном интеллекте*[179] (*Artificial intelligence act, AIA*). Данный регламент был принят в 2024 г.[180]. В соответствии с ним на уровне ЕС был сформирован прогрессивный режим правового регулирования ИИ, основанный на риск-ориентированном подходе. Кроме того, в рамках

---

[178] Order of the President of the General Court of 27 September 2023. Amazon Services Europe Sàrl v European Commission. Case T-367/23 R // ECLI:EU:T:2023:589; Order of the Vice-President of the Court of 27 March 2024. European Commission v Amazon Services Europe Sàrl. Case C-639/23 P(R) // ECLI:EU:C:2024:277.

[179] Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. COM/2021/206 final. Brussels, 21.4.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206 (accessed: 19.12.2022).

[180] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (PE/24/2024/REV/1) // OJ L, 2024/1689, 12.7.2024.

соответствующего регламента были возложены дифференцированные обязанности и ответственность на поставщиков (разработчиков) и пользователей ИИ-систем, создана гармонизированную европейскую систему оценки соответствия, сертификации и регистрации ИИ-систем, а также учреждены специальные наднациональные и национальные органы власти, наделенные полномочиями в сфере регистрации и контроля функционирования ИИ-систем.

При этом стоит отметить, что принятие Регламента об искусственном интеллекте может позволить ЕС стать лидером в соответствующей сфере за счет создания прозрачного и эффективного правового режима ИИ, которого в настоящее время нет ни в одной стране мира (в подобном контексте AIA рассматривается как перспективный инструмент нормативной силы ЕС[181]).

Еще одной новаторской инициативой в части наднационального регулирования цифрового пространства в ЕС стало принятие Регламента о рынках крипто-активов[182] (далее также — MiCA).

В соответствии с данным регламентом обеспечивается включение криптоактивов и крипто-валютных бирж в систему правового регулирования рынка капиталов, а также в сферу платежей. MiCA предполагает внедрение на уровне ЕС требований к минимальному размеру капиталов криптовалютных бирж и эмитентов криптоактивов, к управлению ими, к процедурам аудита и контроля, комплаенса и т.д. Также в рамках MiCA осуществлена дифференциация правового регулирования криптоактивов в зависимости от их типа: обычные криптоактивы, обеспеченные

---

[181] См., например: Саворская Е.В. Сущность концепции «Нормативной силы» Европейского союза // Балт. рег.. 2015. №4. С. 90-104; Игумнова Л.О. Образ нормативной силы Евросоюза в заявлениях Европейской внешнеполитической службы // Современная Европа. 2017. №6 (78). С. 81-93; Степанян А.Ж. Регламент Европейского Союза об искусственном интеллекте (Artificial Intelligence Act): первый взгляд на проект // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. № 7. С. 93-98.

[182] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (PE/54/2022/REV/1) // OJ L 150, 9.6.2023, p. 40–205.

криптоактивы и криптовалюты. В зависимости от типа криптоактива к нему подлежат применению различные требования (также указанные в MiCA). При этом значение принятия MiCA состоит не только в том, что в ЕС планируется создать эффективную правовую базу для регулирования криптоиндустрии (чего фактически нет ни в одном современном правопорядке), но и стать лидером в соответствующей сфере правового регулирования (что позволит использовать MiCA в качестве еще одного инструмента нормативной силы ЕС).

Кроме того, после 2020 г. продолжилось развитие *и сложившихся ранее направлений* наднационального регулирования цифрового пространства в ЕС.

Так, в частности, в соответствии с положениями Европейской стратегии данных[183] предполагается расширение наднационального регулирования порядка обращения неперсональных данных в цифровой среде, развития процесса сбора, анализа и обмена данными, а также создание коммунитарной системы предоставления доступа к неперсональным данным для резидентов Европейского союза (особенно в сфере бизнес-взаимодействий B2B и в сфере взаимодействий граждан с правительствами). Также в соответствии со стратегией закрепляется принцип свободного доступа к отдельным категориям публичных данных государств – членов ЕС и наднациональных институтов ЕС (например, в сфере здравоохранения).

Сегодня в ЕС формируются и наднациональные правовые основы регулирования облачной инфраструктуры. Создание облачной инфраструктуры планируется обеспечить за счет активизации инновационных закупок, совершенствования коммунитарного регулирования порядка обращения неперсональных данных, введения в действие Регламентов о цифровых рынках и о цифровых услугах, создания

[183] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A European strategy for data COM/2020/66 final. Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (accessed: 19.12.2022).

наднациональной правовой базы для развития облачных вычислений. Основой для реализации соответствующей деятельности выступает Европейская стратегия данных[184]. При этом особое внимание здесь уделяется вопросам обеспечения энергоэффективности и снижению выбросов парниковых газов[185], создаваемой и функционирующей цифровой и информационно-коммуникационной инфраструктуры в соответствии с принципами Европейского зеленого пакта[186]. Формирование соответствующего регулятивного механизма было возложено на Еврокомиссию, которая должна разработать и утвердить расширенные индексы цифровой экономики и общества (англ. Digital Economy and Society Index, DESI[187]).

Также в 2020 г. была принята новая Стратегия кибербезопасности ЕС на цифровое десятилетие[188]. В 2021 г. для обеспечения кибербезопасности на уровне ЕС было образовано Объединенное подразделение по кибербезопасности (*англ. Joint Cybersecurity Unit*), которое обеспечило более

---

[184] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A European strategy for data COM/2020/66 final. Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (accessed: 19.12.2022).

[185] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade. COM/2021/118 final. Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 19.12.2022).

[186] Communication from the Commission to the European Parliament, the European council, the Council, the European economic and social committee and the Committee of the regions: The European Green Deal (COM/2019/640 final). Brussels, 11.12.2019 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN (accessed: 19.12.2022).

[187] The Digital Economy and Society Index [Electronic source] // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 19.12.2022).

[188] Joint communication to the European parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade. JOIN(2020) 18 final. Brussels, 16.12.2020 // [Electronic source]. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (accessed: 19.12.2022).

тесную координацию между наднациональными институтами ЕС и органами государственной власти государств-членов ЕС[189].

Для современного этапа развития наднационального регулирования цифрового пространства в ЕС характерно и создание общей коммунитарной основы для осуществления публичных закупок в сферах цифровой и облачной инфраструктуры. Правовой основой тут выступают положения Директивы о государственных закупках, касающиеся особенностей осуществления закупочной деятельности в инновационных сферах. Кроме того, в данной сфере также планируется формирование единой коммунитарной системы публичных закупок, осуществляемых в целях создания, развития и поддержания функционирования цифровой и облачной инфраструктуры[190]. При этом осуществление подобных закупок тесно связано с необходимостью совершенствования наднационального регулирования в сфере обеспечения безопасности подобной инфраструктуры[191].

Таким образом, актуальный этап развития наднационального регулирования цифрового пространства в ЕС характеризуется переходом к формированию принципиально новых масштабных направлений интеграции в цифровой сфере[192].

В целом же, завершая исследование эволюции наднационального правового регулирования цифрового пространства в ЕС, можно сделать вывод о том, что она включает в себя три основных этапа.

---

[189] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. PE/28/2021/INIT // OJ L 202, 8.6.2021, p. 1–31.

[190] Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper). European Court of Auditors. 2019. 74 p.

[191] Madiega T. Digital sovereignty for Europe. European Parliamentary Research Service (EPRS) Ideas Paper. July 2020. 12 p.

[192] Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. 2023. № 1. С. 12-25.

1. тап зарождения регулирования цифрового пространства (2010–2014 гг.). На данном этапе основное внимание было сосредоточено на формировании гармонизированной системы публичных закупок в электронной форме, а также на совершенствовании общеевропейской системы защиты интеллектуальной собственности и авторских прав в сети Интернет (при этом здесь были использованы достаточно нестандартные механизмы мягкого рыночного влияния на участников цифровых рынков за счет принятия ими на себя добровольных обязательств перед правообладателями при посредничестве Еврокомиссии). Тем не менее, несмотря на предпринятые шаги, наднациональное регулирование цифрового пространства все еще носило крайне фрагментарный характер и не затрагивало большого количества сфер цифровой общественной жизни, имеющих принципиальное значение для развития европейской интеграции (в частности, речь здесь идет об отсутствии наднационального регулирования цифровых рынков и цифровых услуг, обращения цифровых данных, кибербезопасности и т.д.).

2. Этап фрагментарного регулирования цифрового пространства (2015–2019 гг.). В рамках данного этапа развития наднационального правового регулирования цифрового пространства в ЕС было обеспечено существенное расширение сфер соответствующего регулирования по сравнению с предыдущим этапом. Так, в частности, в период с 2014 г. по 2019 г. были обеспечены разработка и принятие актов ЕС в сфере защиты и обращения персональных и неперсональных данных, а также в сфере кибербезопасности. При этом принятые в рамках соответствующего этапа Общий регламент по защите данных 2016 г., Регламент в сфере обращения неперсональных данных на территории ЕС 2018 г., Директива по безопасности сетей и информационных систем 2016 г., Регламент о кибербезопасности 2019 г. стали ключевыми актами в соответствующих сферах, сформировав наиболее принципиальные черты правового режима

защиты и обращения данных в сети Интернет, а также обеспечив внедрение современного общеевропейского подхода к обеспечению кибербезопасности.

3. Этап всеобъемлющего регулирования цифрового пространства (2020 г. – н.в.). Данный этап развития наднационального регулирования цифрового пространства в ЕС характеризуется переходом к формированию принципиально новых масштабных направлений интеграции в цифровой сфере. К подобным направлениям, в частности, относятся создание правовой базы для функционирования единого рынка цифровых услуг ЕС, а также для единообразного применения технологий искусственного интеллекта в государствах членах ЕС и для единообразного регулирования рынка крипто-активов. Кроме того, на данном этапе свое углубление и расширение получили и традиционные направления наднационального регулирования цифрового пространства в ЕС в таких сферах, как защита интеллектуальной собственности в сети Интернет, обеспечение кибербезопасности, защита и оборот неперсональных данных, обеспечение стабильности и безопасности цифровой (а именно облачной) инфраструктуры, гармонизация правил осуществления публичных закупок в электронной форме и закупок цифровых товаров и услуг.

§ 2.2. Особенности правового регулирования цифровой инфраструктуры и цифровой среды на уровне ЕС

Регулирование цифровой инфраструктуры и цифровой среды на уровне ЕС достаточно обширно и включает в себя такие традиционные аспекты наднационального правового регулирования общественных отношений в цифровой сфере, как: 1) наднациональное регулирование порядка обращения персональных данных в рамках единого цифрового пространства; 2) наднациональное регулирование порядка доступа к официальной государственной информации и иным неперсональным данным в пространстве интеграционного объединения; 3) наднациональные требования

к надежности, безопасности, устойчивости (прежде всего, экологической) и защищенности информационно-коммуникационной инфраструктуры; 4) наднациональные основы совместного противодействия киберпреступности и кибертерроризму, а также обеспечение кибербезопасности[193].

При этом в 2020 г. в соответствии с Обращением У. фон дер Ляйен[194] и на основе положений Цифрового компаса 2030[195] развитие наднационального регулирования единого цифрового пространства было привязано к разработке нового правового регулирования по трем основным направлениям: 1) цифровая среда; 2) цифровая инфраструктура; 3) цифровой рынок. Таким образом, комплексное правовое регулирование цифровой сферы на уровне ЕС в настоящее время осуществляется в рамках двух основных направлений[196]:

1) совершенствование наднационального регулирования единой цифровой среды в части обеспечения кибербезопасности и защиты персональных данных (Регламент по защите данных 2016 г.[197], Регламент о

---

[193] Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. 2023. № 1. С. 12-25.

[194] State of the Union Address by President von der Leyen at the European Parliament Plenary [Electronic source] // European Commission. 16 September 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (accessed: 20.12.2022).

[195] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 20.12.2022).

[196] Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. 2022. № 1. С. 61–75.

[197] 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) // OJ L 119, 4.5.2016, p. 1–88.

кибербезопасности 2019 г.[198], Директива об обеспечении общего высокого уровня кибербезопасности в Союзе 2022 г.[199]);

2) развитие наднациональных правовых основ единой цифровой (облачной) инфраструктуры (Регламент о свободном обращении неперсональных данных на территории ЕС 2018 г.[200], Европейская стратегия данных 2020. г.[201], требования климатической нейтральности и энергоэффективности[202], индексы цифровой экономики и общества (англ. Digital Economy and Society Index, DESI[203])).

Рассмотрим отмеченные направления более подробно.

Совершенствование наднационального регулирования в части обеспечения кибербезопасности и защиты персональных данных

Первым шагом на пути развития наднационального регулирования цифровой среды на уровне ЕС стало создание наднациональной правовой базы в сфере обеспечения кибербезопасности[204]. Так, в 2013 г. был принят

---

[198] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // OJ L 151, 7.6.2019, p. 15–69.

[199] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (PE/32/2022/REV/2) // OJ L 333, 27.12.2022, p. 80–152.

[200] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union // OJ L 303, 28.11.2018, p. 59–68.

[201] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A European strategy for data (COM/2020/66 final). Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (accessed: 20.12.2022).

[202] Communication from the Commission to the European Parliament, the European council, the Council, the European economic and social committee and the Committee of the regions: The European Green Deal (COM/2019/640 final). Brussels, 11.12.2019 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN (accessed: 20.12.2022).

[203] The Digital Economy and Society Index [Electronic source] // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 20.12.2022).

[204] Лю К.А. Указ. соч. С. 65.

специальный документ —– Стратегия кибербезопасности ЕС[205], в 2016 г. — Директива по безопасности сети и информационных систем[206] (Директива NIS), в 2017 г. — План скоординированного реагирования на крупные кибератаки[207]. Особый всплеск законотворческой активности пришелся на 2018-2019 гг., когда был принят набор законодательных актов в сфере кибербезопасности[208], включающий в себя, в том числе, Регламент о кибербезопасности[209].

Следующим шагом в данном направлении стало принятие в 2016 г. Общего регламента по защите данных[210], а на современном этапе ключевой задачей в рамках реализации данного направления формирования единого цифрового пространства ЕС является разработка и внедрение новых стандартов регулирования и контроля цифровых продуктов и услуг. При этом данные стандарты должны распространяться как на внутренних (резиденты ЕС), так и на внешних участников цифрового рынка. Создание отмеченных стандартов в настоящее время ведется в рамках двух основных сфер: 1) в сфере кибербезопасности и 2) в сфере защиты персональных данных в цифровой среде[211].

---

[205] Joint communication to the European Parliament, the Council, the European economic and Social Committee and the Committee of the regions «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace» // JOIN (2013) 1 final. Brussels, 7.2.2013.

[206] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // OJ L 194, 19.7.2016, p. 1–30.

[207] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises // OJ L 239, 19.9.2017, p. 36–58.

[208] Joint Communication to the European Parliament and the Council «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU» // JOIN/2017/0450 final.

[209] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // OJ L 151, 7.6.2019, p. 15–69.

[210] 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) // OJ L 119, 4.5.2016, p. 1–88.

[211] Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. 2022. № 1. С. 61–75.

Совершенствование наднационального правового регулирования в сфере кибербезопасности включает в себя три ключевых направления развития наднациональной нормативной базы[212].

Во-первых, в настоящее время ведется работа по совершенствованию системы сертификации в сфере кибербезопасности, которая бы обеспечивала надежную защиту потребителей и бизнеса в цифровой среде. При этом новые стандарты сертификации были приняты в 2023 г. Общей нормативной основой для внедрения данных стандартов стало внесение изменений[213] в Директиву об обеспечении общего высокого уровня кибербезопасности в Союзе[214].

Во-вторых, достижение уровня кибербезопасности, необходимого для формирования единого цифрового пространства, требует устранения пробелов и коллизий, существующих в праве ЕС в части требований к обеспечению кибербезопасности. Как отмечается в отчете Европейской счетной палаты[215], подобные правовые лакуны в настоящее время присутствуют в рамках регулирования компетенции ЕС и государств-членов в сфере кибербезопасности, а также в сфере наднациональных требований к раскрытию киберрисков.

В-третьих, построение единого цифрового рынка в ЕС на сегодняшний день также предполагает разработку и принятие наднациональных требований к обеспечению кибербезопасности публичных закупок объектов, работ и услуг, связанных с построением цифровой и облачной инфраструктуры как на уровне ЕС, так и на национальном уровне. Кроме

---

[212] Там же. С. 66.

[213] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) // OJ L 333, 27.12.2022, p. 80–152.

[214] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (PE/32/2022/REV/2) // OJ L 333, 27.12.2022, p. 80–152.

[215] Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper). European Court of Auditors. 2019.

того, здесь ставится и более общая задача по совершенствованию системы кибербезопасности публичных закупок в целом, которая должна учитывать актуальные вызовы и критические аспекты внедрения цифровых технологий в чувствительных секторах экономики[216]. Более того, в настоящее время Европейская счетная палата уже подготовила предложение о создании системы общих публичных закупок для создания цифровой и облачной инфраструктуры в масштабах всего Европейского союза[217], что является еще одним важным шагом к формированию надежной и безопасной цифровой среды, а, следовательно, и единого цифрового пространства ЕС.

Защита персональных данных в цифровой среде представляет собой вторую актуальную составляющую деятельности ЕС в сфере построения надежной и безопасной цифровой среды[218].

Нормативное регулирование защиты персональных данных на наднациональном уровне в ЕС на текущем этапе преимущественно сосредоточено вокруг положений GDPR, о полной имплементации которых в национальные правопорядки государств-членов Еврокомиссия отчиталась в июне 2020 г.[219]

Однако пандемия коронавируса выявила серьезные недостатки регулирования, содержащиеся в данном акте. Ключевой проблемой здесь является тот факт, что в настоящее время основными субъектами сбора, хранения и анализа больших данных (в т.ч. персональных) выступают компании, инкорпорированные в США (т.н. GAFAM —– Google, Apple, Facebook, Amazon и Microsoft) и в Китае. Подобная ситуация влечет за собой фактическую утрату контроля над обращением с персональными данными

---

[216] Madiega T. Op. cit. P. 9.
[217] Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper). European Court of Auditors. 2019. P. 54.
[218] Лю К.А. Указ. соч. С. 67.
[219] Commission report: EU data protection rules empower citizens and are fit for the digital age // [Electronic source] // European Commission. 24 June 2020. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018PC0630 (accessed: 20.12.2022).

граждан ЕС[220]. Как следствие, в большинстве случаев использования персональных данных для отслеживания социальных контактов в период пандемии наднациональное европейское регулирование оказывалось неприменимо. При этом подобная ситуация существовала уже довольно длительное время. Пандемия китайского коронавируса лишь более ярко осветила ее наличие[221].

Таким образом, необходимость совершенствования наднациональной системы защиты персональных данных в ЕС стала рассматриваться в качестве неотъемлемого элемента стратегии по формированию единого цифрового пространства[222]. В настоящее время ведется работа по созданию и принятию стандартов и инструкций в сфере усиленной защиты персональных данных в наиболее чувствительных сферах общественной жизни (финансовом секторе, здравоохранении и др.), однако к 2030 г. планируется полностью модернизировать систему защиты персональных данных таким образом, чтобы она обеспечивала высокий уровень защиты данных и конфиденциальности вне зависимости от конкретных обстоятельств хранения и обработки таких данных[223].

Развитие наднациональных правовых основ единой цифровой (облачной) инфраструктуры

Создание безопасной, высокопроизводительной и устойчивой цифровой инфраструктуры воспринимается в ЕС в качестве неотъемлемого условия для формирования единого цифрового пространства. При этом в состав деятельности по формированию современной и эффективной цифровой инфраструктуры в ЕС входят два направления: 1) обеспечение

[220] Madiega T. Op. cit. P. 10.
[221] Лю К.А. Указ. соч. С. 67.
[222] Лю К.А. Указ. соч. С. 67.
[223] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 20.12.2022).

свободного высокоскоростного подключения к сети Интернет на территории всего Европейского союза и 2) развитие внутриевропейских инициатив в сфере сбора, хранения и обработки больших данных (англ. big data)[224].

В рамках первого направления в настоящее время в ЕС поставлена задача по обеспечению гигабитной связи на всей территории Европейского союза к 2030 г. При этом основное внимание здесь предполагается уделить созданию устойчивого, фиксированного мобильного и спутникового подключения на базе создания сетей с очень высокой пропускной способностью (5G на текущем этапе с потенциалом развертывания сетей 6G к 2030 г.). Главной целью здесь является обеспечение охвата гигабитными сетями всех населенных пунктов ЕС к 2030 г.[225]

Второе направление предполагает развитие собственных внутриевропейских мощностей (в т.ч. за счет созданию выгодных условий для бизнеса) в сфере хранения и обработки больших данных в целях возвращения мест хранения данных резидентов ЕС на территории Европейского союза (в настоящее время большие данные европейцев хранятся в рамках структур крупнейших американских и китайских IT-гигантов[226]). Иными словами, в настоящее время ЕС нацелен на формирование собственной наднациональной облачной инфраструктуры сбора, хранения и обработки данных резидентов ЕС, национальных органов власти государств – членов ЕС и наднациональных органов ЕС[227].

---

[224] Лю К.А. Указ. соч. С. 68.
[225] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 20.12.2022).
[226] Madiega T. Op. cit.
[227] Лю К.А. Указ. соч. С. 68.

С этой целью в 2018 г. был принят Регламент о свободном обращении неперсональных данных на территории ЕС[228], которым были установлены правила хранения и обработки соответствующих данных на облачных серверах, физически расположенных на территории ЕС, а также правила доступа государственных органов к таким данным (правила электронного документооборота и оборота неперсональных данных). При этом стратегической целью принятия данного регламента выступало стремление создать правовую базу для наднационального регулирования облачных вычислений в целом[229].

Сегодня нормативной основой реализации мероприятий в рамках данного направления являются положения Европейской стратегии данных[230], которая предполагает разработку и принятие новых регулятивных мер в сфере внедрения облачной инфраструктуры в масштабах всего Европейского союза.

Отдельное внимание уделяется вопросам снижения объемов потребления энергии объектами цифровой и облачной инфраструктуры. В частности, в соответствии с Цифровым компасом – 2030 устанавливается, что подобная инфраструктура к 2030 г. должна соответствовать принципам климатической нейтральности и энергоэффективности[231]. При этом избыточная энергия будет направляться на цели обогрева жилых домов, коммерческих зданий и мест общественного пользования. Формирование

---

[228] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union // OJ L 303, 28.11.2018, p. 59–68.

[229] Лю К.А. Указ. соч. С. 68.

[230] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A European strategy for data (COM/2020/66 final). Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (accessed: 20.12.2022).

[231] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 20.12.2022).

соответствующего регулятивного механизма было возложено на Еврокомиссию, которая должна разработать и утвердить расширенные индексы цифровой экономики и общества (англ. Digital Economy and Society Index, DESI[232]).

В целом, поводя итог настоящему параграфу, можно еще раз отметить следующее:

в рамках первого направления были разработаны и внедрены новые стандарты кибербезопасности и обращения с персональными данными на уровне ЕС. При этом данные стандарты распространяются как на внутренних (резидентов ЕС), так и на внешних участников цифрового рынка. Общей нормативной основой для внедрения новых стандартов кибербезопасности стало внесение изменений в Директиву о безопасности сетей и информационных систем 2016 г. В части защиты персональных данных в цифровой среде сегодня ведется работа по созданию и принятию стандартов и инструкций в сфере усиленной защиты персональных данных в наиболее чувствительных сферах общественной жизни (финансовом секторе, здравоохранении и др.), а к 2030 г. планируется полностью модернизировать систему защиты персональных данных таким образом, чтобы она обеспечивала высокий уровень защиты данных и конфиденциальности вне зависимости от конкретных обстоятельств хранения и обработки таких данных[233];

второе направление представлено преимущественно положениями Европейской стратегии данных 2020 г., устанавливающей необходимость разработки и принятия наднациональных правил создания и функционирования облачной инфраструктуры, которые бы обеспечили создание конкурентных условий сбора, анализа, обработки и обмена неперсональными данными для резидентов ЕС. При этом в основу такого

[232] The Digital Economy and Society Index [Electronic source] // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 20.12.2022).
[233] Лю К.А. Указ. соч. С. 73.

регулирования положен принцип открытого доступа к государственным и наднациональным данным в отдельных стратегических секторах (в частности, в сфере транспорта и здравоохранения). Кроме того, в сферу правового регулирования цифровой инфраструктуры были инкорпорированы требования обеспечения нулевого уровня выбросов парниковых газов и энергоэффективности посредством возложения на Еврокомиссию обязанности разработать новые расширенные индексы цифровой экономики и общества (DESI)[234].

§ 2.3. Особенности правового регулирования цифрового рынка и цифровых услуг на уровне ЕС

Создание наднациональных правовых основ единого цифрового рынка, порядка доступа на рынок и осуществления деятельности на нем различными субъектами, специальных антимонопольных правил, правового режима защиты прав потребителей и иных регуляторных требований в соответствующих сферах стало третьим направлением развития наднационального регулирования цифрового пространства в ЕС, которое было определено в соответствии с Обращением У. фон дер Ляйен и на основе положений Цифрового компаса – 2030.

При этом правовое регулирование цифрового рынка ЕС и рынка цифровых услуг представляет собой наиболее новое направление наднационального регулирования цифрового пространства, которое до 2020 г. (а точнее, до 2022 г., когда были приняты регламенты DSA и DMA) в ЕС не существовало.

2.3.1. Наднациональное регулирование цифровых услуг

Несмотря на то, что детальное наднациональное регулирование предоставления цифровых услуг на единых рынках ЕС было установлено

[234] Там же.

только в рамках DSA, определение цифровых услуг в правопорядке ЕС было сформулировано еще в 2015 г. в Директиве об услугах информационного общества[235] (далее также — Директива 2015/1535). Именно на положения данной директивы ссылается DSA при описании категории «цифровые услуги».

При этом сама Директива об услугах информационного общества не содержала в себе наднационального регулирования цифровых услуг. Она лишь предусматривала формирование специализированного консультативного Комитета по техническому регулированию цифровых услуг, основной задачей которого являлось содействие государствам-членам в согласовании технических регламентов в целях избежания барьеров на внутренних рынках, а также содействие гармонизации технического регулирования услуг информационного общества.

В соответствии с пп. b ч. 1 ст. 1 Директивы 2015/1535 устанавливается, что услуги информационного общества (цифровые услуги) представляют собой услуги, которые на возмездной основе по запросу со стороны заказчика предоставляются ему дистанционно с использованием электронных средств. Таким образом, конститутивными признаками цифровых услуг в правопорядке ЕС являются: 1) предоставление услуг с использованием электронных средств; 2) предоставление услуг дистанционно; 3) предоставление услуг по запросу заказчика.

Предоставление цифровых услуг с использованием электронных средств, согласно Директиве 2015/1535, подразумевает, что такие услуги предоставляются и принимаются с использованием электромагнитных средств передачи данных. При этом, как указано в Приложении № 1 к Директиве 2015/1535, не могут квалифицироваться в качестве услуг, предоставляемых с использованием электронных средств а) услуги с

[235] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) // OJ L 241, 17.9.2015, p. 1–15.

материальным содержанием, которые оказываются с использованием электронных устройств (например, реализация материальных товаров в сети Интернет); б) услуги, которые предоставляются лично заказчику на физических цифровых носителях (на дисках, картах памяти и др.); в) услуги, которые предоставляются по телефонной связи или посредством телефакса.

В свою очередь, предоставление цифровых услуг дистанционно означает, что лицо, предоставляющее услугу, и заказчик услуги при заключении и исполнении договора не находятся в одном и том же месте. Если предоставление услуг предполагает присутствие заказчика и исполнителя одновременно в одном месте, то такие услуги не могут квалифицироваться в качестве цифровых. Иными словами, в правопорядке ЕС не будут являться цифровыми услуги по онлайн-бронированию билетов в кассах и терминалах или в офисах туристических агентств, услуги по предоставлению доступа к компьютерному оборудованию для работы или развлечений и т.д.

Наконец, предоставление цифровых услуг по запросу заказчика предполагает персональный характер данных услуг. Цифровые услуги должны предоставляться на индивидуальные устройства заказчика услуг по его запросу.

Таким образом, цифровые услуги в правопорядке ЕС представляют собой возмездные услуги, которые не имеют материального содержания и предоставляются по индивидуальному запросу заказчика дистанционно посредством цифровых средств передачи данных без использования физических цифровых носителей и без присутствия исполнителя и заказчика одновременно в одном месте.

Впрочем, DSA распространяется не на все цифровые услуги. Сфера действия данного регламента сужена и ограничивается только теми

цифровыми услугами, которые носят посреднический характер[236]. На соответствующее ограничение прямо указано в ч. 1 ст. 1 Регламента, в соответствии с которой устанавливается, что он ориентирован на внутренний рынок цифровых посреднических услуг ЕС.

При этом к подобным цифровым посредническим услугам отнесены три типа услуг (п. g ст. 3 DSA):

- просто проводник (англ. mere conduit) — цифровая посредническая услуга, где исполнитель принимает на себя обязательства по передаче цифровых данных (информации) заказчика через информационно-коммуникационную сеть или обязательства по предоставлению доступа такой сети для заказчика;

- кэширование (англ. caching) —– цифровая посредническая услуга, в рамках которой исполнитель принимает на себя обязательства по передаче цифровых данных заказчика, а также обязательства по их временному хранению в целях увеличения эффективности передачи данных, полученных от заказчика;

- хостинг (англ. hosting) — цифровая посредническая услуга, в рамках которой исполнитель принимает на себя обязательства по хранению цифровых данных, предоставленных заказчиком, а также по предоставлению полученных данных по запросу заказчика.

На базе данных трех типов цифровых посреднических услуг DSA обеспечивает наднациональное регулирование деятельности интернет-провайдеров, онлайн-поисковиков, социальных сетей, маркетплейсов, а также иных IT-компаний, которые предоставляют посреднические цифровые услуги (в виде передачи и хранения цифровых данных) потребителям на территории ЕС[237].

---

[236] Chiarella M.L. Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment // Athens Journal of Law. 2022. № 9. P. 1-25.

[237] Heldt A. EU Digital Services Act: The White Hope of Intermediary Regulation // in: Digital Platform Regulation. Global Perspectives on Internet Governance / T. Flew, F.R. Martin (eds). Palgrave Macmillan, 2022. P. 69-84.

Впрочем, ввиду широты сферы действия DSA по кругу субъектов потребовалось дробление правового режима предоставления цифровых посреднических услуг по степени и характеру обязанностей.

Так, универсальный правовой режим, устанавливающий базовые требования для всех поставщиков цифровых посреднических услуг, в качестве одного из основных обязательств возлагает на них обязанность удалять не соответствующий законодательству цифровой контент и предоставлять определенную информацию по запросу со стороны органов власти государств-членов и со стороны уполномоченных институтов ЕС (ст. 8, ст. 9 DSA)[238]. Однако обязанность по инициативному выявлению подобного цифрового контента на поставщиков цифровых посреднических услуг в рамках универсального правового режима не возлагается.

Таким образом, данное требование призвано сформировать правовую основу для взаимодействия органов публичной власти и поставщиков цифровых посреднических услуг, а также обеспечить возможность удаления противоправного цифрового контента в административном порядке (без обращения в суд), что особенно важно для институтов ЕС, которые могут направлять соответствующие запросы напрямую цифровым посредникам без привязки их деятельности к конкретным национальным правопорядкам. В соответствующих целях ст. 11 DSA налагает на поставщиков цифровых услуг обязанность назначить единое контактное лицо.

Помимо отмеченных обязанностей на всех лиц, предоставляющих посреднические цифровые услуги, распространяются требования в сфере создания прозрачной и справедливой онлайн-среды. Соответствующие требования предполагают:

- создание механизмов обратной связи (включая единое контактное лицо) посредством которых пользователи могут оперативно в электронной форме связаться с цифровыми поставщиками (ст. 12 DSA);

---

[238] Church P., Pehlivan C.N. The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability // Global Privacy Law Review. 2023. Vol. 4. Is. 1. P. 53-59.

- полное раскрытие информации о существующих ограничениях при использовании цифровых сервисов, в т.ч. в части типа и характера допускаемого к распространению цифрового контента, а также порядка использования цифровых сервисов (ст. 14 DSA);

- ежегодную публикацию данных об удалении, изменении или блокировке цифрового контента (ст. 15 DSA).

В целом универсальный правовой режим предполагает возложение на цифровых посредников двух групп обязанностей, связанных с обеспечением эффективной связи с органами публичной власти, с одной стороны, и с пользователями цифровых сервисов, с другой стороны. Именно вокруг данных двух групп обязанностей сконструирован универсальный правовой режим. Требования иного характера устанавливаются уже в рамках более строгих правовых режимов.

Так, правовой режим хостинга (который также может быть обозначен как дополненный правовой режим) содержит в себе три дополнительных группы обязанностей:

- создание механизмов, предоставляющих пользователям цифровых сервисов возможность направлять уведомления о выявленном ими цифровом контенте, который нарушает требования законодательства (ст. 16 DSA);

- обязательное уведомление пользователей цифровых сервисов о причинах удаления, блокировки, ограничения доступа или введения иных ограничительных мер (например, ограничения монетизации) в отношении размещаемого ими цифрового контента (ст. 17 DSA);

- обязательное направление сообщений о выявленной в цифровом контенте информации о совершении или о подготовке к совершению преступления против безопасности, здоровья или жизни (ст. 18 DSA).

В свою очередь, правовой режим онлайн-платформ предполагает возложение на поставщиков цифровых посреднических услуг еще большего количества обязанностей.

При этом соответствующий правовой режим распространяется только на оказание услуг онлайн-платформы, под которыми в соответствии со ст. 3 DSA понимаются цифровые услуги по хранению и публичному распространению цифрового контента (цифровой информации) пользователей по их индивидуальному запросу. Оказание соответствующих цифровых услуг должно быть основным видом деятельности поставщика таких услуг. Одновременно из-под действия данного правового режима выведены все субъекты микро- и малого предпринимательства, даже если они в качестве основного направления деятельности предоставляют цифровые услуги онлайн-платформы (ст. 19 DSA).

К числу особых обязанностей поставщиков цифровых услуг онлайн-платформ (в дополнение ко всем отмеченным выше обязанностям, предусмотренным универсальным и дополнительным правовыми режимами) относятся:

1) обязанности в сфере противодействия распространению незаконного цифрового контента:

- обязанность по созданию механизма независимого мониторинга и выявления незаконного цифрового контента, размещаемого на онлайн-платформах, в форме деятельности сертифицированных Координатором цифровых услуг государства-члена доверенных осведомителей (англ. trusted flaggers) (ст. 22 DSA);

- обязанность по приостановке предоставления цифровых услуг онлайн-платформы пользователям, систематически размещающим незаконный цифровой контент (ст. 23 DSA).

2) обязанности по формированию прозрачной и справедливой онлайн-среды:

- обязанность по созданию внутренней системы реагирования на претензии со стороны пользователей (создание механизма обратной связи в виде единого контактного лица и доведение до пользователей информации о

причинах введенных в отношении их контента ограничений уже недостаточно для онлайн-платформ) (ст. 20 DSA);

- обязанность по добросовестному взаимодействию с пользователями онлайн-платформ, которая предполагает отказ от использования манипулятивных технологий, методов ограничения возможностей пользователей по бесплатному и информированному использованию онлайн-платформ (в т.ч. в рамках дизайна и функционала собственного онлайн-интерфейса) (ст. 25 DSA);

- обязанность по полному раскрытию информации о материалах рекламного характера, размещаемых на онлайн-платформах, включая указание на рекламный характер цифрового контента, информацию о рекламодателе, информацию о причинах демонстрации таргетированных рекламных объявлений и др. При этом установлен прямой запрет на использование для таргетирования рекламы персональных данных пользователей, которые GDPR квалифицируются как специальные (персональные данные о расе, этносе, биометрические данные, генетические данные, политические убеждения, религиозные взгляд и др. (ст. 26 DSA)).

При этом специальный правовой режим онлайн-платформ, распространяющийся на маркетплейсы (онлайн-платформы, опосредующие дистанционную онлайн-торговлю с участием потребителей), содержит в себе специальные обязанности, связанные со спецификой именно торговой деятельности.

Так, в частности, маркетплейсы как поставщики цифровых посреднических услуг в соответствии с положениями DSA обязаны:

- обеспечивать сбор, верификацию и доведение до сведения потребителей информации о продавцах-пользователях онлайн-платформы (к такой информации отнесены сведения о наименовании, месте регистрации и ведения деятельности, контактных данных, о включении в публично достоверные реестры, о сертификации) (ст. 30 DSA);

- обеспечивать сбор и верификацию (но не публичное размещение) документов, удостоверяющих личность продавцов-пользователей онлайн-платформ, а также данных о платежных счетах продавцов (ст. 30 DSA);

- разрабатывать дизайн и функционал онлайн-платформ так, чтобы продавцы-пользователи могли свободно и в полном объеме исполнять обязанности по доведению до потребителей всей необходимой информации в соответствии с законодательством о защите прав потребителей (ст. 31 DSA);

- при обнаружении фактов реализации товаров, не соответствующих требованиям законодательства, доводить до сведения всех лиц, купивших такие товары, информацию о выявленных нарушениях закона, о продавце, а также о способах возмещения ущерба (ст. 32 DSA).

Несение соответствующих специальных обязанностей возложено на все маркетплейсы за исключением субъектов микро- и малого предпринимательства (ст. 29 DSA).

Что же касается правового режима особо крупных онлайн-платформ и онлайн-поисковиков, то он основан уже на принципиально ином подходе, ориентированном на предотвращение системных рисков в цифровом пространстве в целом (на что прямо указывается в наименовании Раздела 5 DSA). На соответствующих цифровых посредников возлагаются обязанности системного характера, которые призваны обеспечить соблюдение широких интересов государства и общества[239].

При этом в соответствии со ст. 3 DSA под онлайн-поисковиками (англ. online search engine) понимаются цифровые посреднические услуги, в рамках которых пользователям предоставляется право осуществлять широкий поиск по определенному запросу (сформулированному в текстовом, графическом или аудио-формате) на всех веб-сайтах в сети Интернет (или веб-сайтах на определенных языках). Таким образом, DSA отдельно выделяет

[239] Staab P., SieronS., Piétron D. Counter-Hegemonic Neoliberalism: Making Sense of EU Platform Regulation // Weizenbaum Journal of the Digital Society. 2022. № 2(1). P. 1-18.

соответствующие цифровые услуги и признает за ними особую системную значимость для цифрового пространства.

В соответствии с ч. 1 ст. 33 DSA для квалификации онлайн-платформ и онлайн-поисковиков в качестве особо крупных количество их ежемесячных пользователей должно превышать 45 миллионов (на территории ЕС). Однако закрепление соответствующего правового статуса за цифровыми посредниками происходит не автоматически, а на основании решения Еврокомиссии. Принятие такого решения осуществляется на основе предоставляемой онлайн-платформами и онлайн-поисковиками отчетной документации о своей деятельности, или в отсутствие соответствующей документации — по усмотрению Еврокомиссии. Снятие правового статуса также осуществляется Еврокомиссией, если число ежемесячных пользователей из ЕС на протяжении года составляло менее 45 млн человек.

После квалификации онлайн-платформы или онлайн-поисковика в качестве особо крупных на них возлагаются следующие обязанности системного характера:

- обязанность осуществлять мониторинг и выявление системных рисков в цифровом пространстве, связанных с распространением незаконного цифрового контента; с потенциальным или реальным нарушением прав человека, с угрозами для их защищенности и гарантированности в понимании Хартии ЕС об основных правах; с нарушением прав несовершеннолетних и с угрозами и рисками для их физического и психологического здоровья; а также с нарушением избирательных прав граждан и с угрозами для демократических процессов (ст. 34 DSA);

- обязанность минимизировать отмеченные выше системные риски посредством мониторинга собственных подходов к дизайну и функционалу онлайн-платформ и онлайн-поисковиков; к маркетинговой политике; к модерации цифрового контента; к обращению персональных и

неперсональных данных; к использованию вычислительных мощностей (ст. 35 DSA);

- обязанность принимать участие в разрешении кризисных ситуаций, в рамках которых существуют реальные или потенциальные угрозы для общественной безопасности и здоровья, а также направлять Еврокомиссии отчеты о принятых мерах для преодоления кризисных ситуаций (ст. 36 DSA).

В целом особо крупным онлайн-платформам и онлайн-поисковикам надлежит принимать непосредственное участие в выявлении и устранении практически любых системных рисков, возникающих в цифровом пространстве, чем существенно отличается распространяющийся на них правовой режим от иных правовых режимов предоставления посреднических цифровых услуг.

Таким образом, исходя из анализа положений DSA, можно сделать вывод о существовании пяти подрежимов правового регулирования порядка предоставления цифровых посреднических услуг в ЕС:

1) универсальный правовой режим — набор ограничений, обязанностей и требований к организации предоставления цифровых посреднических услуг, который распространяется на всех цифровых посредников;

2) правовой режим хостинга — дополнительный набор ограничений, обязанностей и требований, распространяющийся на поставщиков цифровых услуг типа «хостинг»;

3) правовой режим онлайн-платформ — набор особых требований, предъявляемых к организации деятельности онлайн-платформ;

4) специальный правовой режим онлайн-платформ — набор специальных требований, соблюдение которых является обязательным для онлайн-платформ, посредством которых обеспечивается онлайн-торговля с участием потребителей;

5) правовой режим особо крупных онлайн-платформ и онлайн-поисковиков — данный режим подлежит применению к цифровым

посредникам, деятельность которых оказывает влияние на предоставление цифровых услуг на системном уровне и несет в себе системные риски для цифрового пространства.

Система приведенных правовых режимов построена по принципу поэтапного усложнение и дополнения: на каждом новом уровне к ограничениям, обязанностям и требованиям, предусмотренным универсальным правовым режимом, добавляются новые.

2.3.2. Наднациональное регулирование цифровых рынков

Наднациональное регулирование цифровых рынков в ЕС в настоящее время осуществляется в соответствии с DMA. При этом основной категорией в рамках соответствующего регламента является «компания-привратник», или цифровой привратник[240].

Частично соответствующая категория может восприниматься как усложненный (квалифицированный) правовой режим осуществления деятельности особо крупными онлайн-платформами и онлайн-поисковиками (которые также могут квалифицироваться в качестве цифровых привратников)[241]. Однако правовой режим цифровых привратников распространяется на более широкий круг субъектов: ими могут быть признаны любые крупные цифровые компании, которые в своей деятельности оказывают или могут оказать существенное влияние на единый рынок цифровых услуг ЕС[242].

---

[240] Colangelo G. DMA begins // Journal of Antitrust Enforcement. 2023. Vol. 11. Is. 1. P. 116–122.

[241] Dickinson I. The quest for a fair price in the digital world - Frand in the DMA 2022. Frontier Economics. United Kingdom, 2022. 6 p.

[242] Davola A., Malgieri G. Data, Power and Competition Law: The (Im)Possible Mission of the DMA? // Research in Law and Economics. 2023. Vol. 31. P. 53-74.

Для квалификации в качестве цифрового привратника компания цифрового сектора должна соответствовать определенным качественным и количественным критериям[243].

Качественные критерии находят свое закрепление в ч. 1 ст. 3 DMA, в соответствии с которой установлено, что для признания компании, предоставляющей цифровые услуги, цифровым привратником необходимо, чтобы она одновременно 1) оказывала существенное влияние на единый рынок определенных цифровых услуг ЕС (или на единый рынок цифровых услуг ЕС в целом); 2) занимала прочное положение на определенном рынке цифровых услуг с сохранением соответствующего положения в будущем; 3) предоставляла услуги основной цифровой платформы (англ. core platform service).

При этом под услугами основной цифровой платформы понимаются услуги, в рамках которых обеспечивается онлайн-взаимодействие между конечными потребителями (конечными пользователями цифровых услуг) и субъектами предпринимательской деятельности (бизнес-пользователями услуг основной платформы)[244]. К услугам основной цифровой платформы, согласно ч. 2 ст. 2 DMA, относятся посреднические цифровые услуги; услуги онлайн-поисковиков; услуги в форме социальных сетей; услуги онлайн-платформ по размещению цифрового видео-контента; услуги личной связи, предоставляемые онлайн без номер телефона; услуги операционных систем; услуги веб-браузеров; услуги виртуальных онлайн-помощников; услуги облачных вычислений; рекламные услуги.

В свою очередь, количественные критерии, закрепленные в ч. 2 ст. 3 DMA, дополняют отмеченные выше качественные критерии следующим образом:

---

[243] Daems I. The complexity and practical challenges of implementing the new DMA // Competition Law & Policy Debate. 2022. № 7(3). P. 106-112.

[244] Gallagher N., Abecasis P. The DMA and the role of economics // Competition Law & Policy Debate. 2022. № 7(3). P. 113-120.

1) существенное влияние на единый рынок определенных цифровых услуг присутствует, если компания предоставляет определенные цифровые услуги в трех или более странах ЕС, либо ее годовой оборот составляет не менее 7,5 млрд евро на протяжении последних трех лет на территории ЕС; либо ее рыночная стоимость составляет не менее 75 млрд евро в последнем финансовом году;

2) оказание услуг основной цифровой платформы требует, чтобы на территории ЕС у компании было не менее 45 млн конечных пользователей (потребителей) и не менее 10 тыс. субъектов предпринимательской деятельности (поставщиков товаров и услуг, пользующихся услугами основной цифровой платформы);

3) прочное положение на определенном рынке цифровых услуг требует сохранения на протяжении не менее трех лет 45 млн конечных пользователей и 10 тыс. субъектов предпринимательской деятельности, пользующихся услугами цифрового привратника.

Таким образом, под цифровыми привратниками в соответствии с DMA понимаются компании с годовым оборотом не менее 7,5 млрд евро или с рыночной стоимостью не менее 75 млрд евро, предоставляющие на территории трех или более государств – членов ЕС (существенное влияние) услуги основной цифровой платформы, посредством которых обеспечивается взаимодействие между 45 млн и более конечными пользователями (потребителями) и 10 тыс. и более бизнес-пользователями (поставщиками) на протяжении не менее трех лет (прочное положение).

При этом в соответствии с положениями DMA компании цифрового сектора, которые удовлетворяют всем отмеченным выше критериям, обязаны самостоятельно в инициативном порядке сообщать Еврокомиссии о наличии качественных и количественных признаков для квалификации в качестве цифровых привратников. В случаях, когда такое сообщение от компании не поступает, Еврокомиссия направляет запрос о предоставлении

корпоративной отчетности о ежегодном доходе, рыночной стоимости, количестве конечных пользователей и бизнес-пользователей, а также о сфере предоставления услуг основной цифровой платформы. Если компания цифрового сектора не предоставляет отчетности по требованию Комиссии, то ЕК вправе квалифицировать ее как цифрового привратника с опорой на информацию о ее деятельности, доступную публично. В последнем случае для снятия правового статуса цифрового привратника компания должна предоставить Комиссии доказательства отсутствия в ее деятельности одного из количественных критериев.

Однако, как указано в ч. 8 ст. 3 DMA, Еврокомиссия вправе по своему усмотрению[245] квалифицировать определенную компанию в качестве цифрового привратника даже в тех случаях, когда один из количественных критериев не выполняется (а все качественные критерии присутствуют). При этом, как следует из конструкции количественных критериев, если не выполняется количественный критерий предоставления услуг основной цифровой платформы (45 млн конечных пользователей и 10 тыс. бизнес-пользователей), то автоматически не выполняется и количественный критерий прочного положения на рынке цифровых услуг (сохранение отмеченных количественных показателей на протяжении трех лет).

Соответственно, положения ч. 8 ст. 3 DMA предоставляют Комиссии право не применять либо количественный критерий существенного влияния на единый рынок (деятельность на территории трех государств – членов ЕС, годовой оборот 7,5 млрд евро или рыночная стоимость 75 млрд евро), либо количественный критерий прочного положения (сохранение определенного числа конечных пользователей и бизнес-пользователей на протяжении трех лет). Иными словами, DMA предполагает предоставление Комиссии

[245] Hoffmann J., Herrmann L., Kestler L. Gatekeeper's Potential Privilege – the Need to Limit DMA Centralisation // Journal of Antitrust Enforcement. Vol. 12. Is. 1. P. 126-147.

достаточно широких дискреционных полномочий[246] по квалификации определенных компаний цифрового сектора в качестве цифровых привратников даже в тех случаях, когда они не в полной мере соответствуют количественным критериям, установленным DMA.

Отмеченная особенность достаточно явно свидетельствует о намерении ЕС сконцентрировать основные контрольно-надзорные полномочия и полномочия по регулированию деятельности цифровых привратников на интеграционном уровне. Именно Еврокомиссия становится ключевым институтом, уполномоченным взаимодействовать с мировыми IT-гигантами, осуществляющими свою деятельность в виде основных цифровых платформ на территории ЕС[247].

Что же касается обязанностей цифровых привратников, то они носят достаточно обширный и разветвленный характер. В рамках DMA выделяется несколько групп обязанностей цифровых привратников применительно к конечным пользователям (потребителям), к бизнес-пользователям (поставщикам), а также применительно к другим участникам цифровых рынков, где ведет свою деятельность цифровой привратник (антимонопольные требования).

Обязанности цифровых привратников в части организации взаимодействия и предоставления услуг основной цифровой платформы конечным пользователям находят свое закрепление в ст. 5 DMA, в соответствии с которой устанавливается следующая система запретов:

- запрет на обработку в рекламных целях персональных данных конечных пользователей (потребителей), которые пользуются основной цифровой платформой для приобретения услуг третьих лиц (бизнес-пользователей);

---

[246] Andriychuk O. Do DMA obligations for gatekeepers create entitlements for business users? // Journal of Antitrust Enforcement. 2023. Vol. 11. Is. 1. P. 123–132.

[247] Or B., Magali E. Who should guard the gatekeepers: does the DMA replicate the unworkable test of Regulation 1/2003 to settle conflicts between EU and national laws? // CPI Antitrust Chronicle. 2022. № 12. P. 37-42.

- запрет на объединение и перекрестное использование персональных данных конечных пользователей, которые были ими предоставлены в рамках получения разных по своему характеру и направлению услуг основной цифровой платформы (например, не допускается объединение персональных данных конечных пользователей, которые были ими предоставлены компании Meta[248] в рамках использования Instagram, WhatsApp и Facebook);

- запрет на объединение персональных данных конечных пользователей с их персональными данными, которые были получены от третьих лиц;

- запрет на автоматическую регистрацию конечных пользователей в дополнительных сервисах основной цифровой платформы на базе единого цифрового аккаунта в целях объединения персональных данных (подобная регистрация является допустимой только в тех случаях, когда пользователи прямо предоставляют свое согласие на обработку персональных данных в дополнительных сервисах);

- запрет на повторное направление запроса о предоставлении согласия на обработку персональных данных для их объединения в рамках единого аккаунта в течение года с момента направления предыдущего запроса.

В целом все обязанности цифровых привратников в части их взаимодействия с конечными пользователями оказываются связаны с обработкой и использованием их персональных данных.

В свою очередь, обязанности цифровых привратников по отношению к бизнес-пользователям основной цифровой платформы носят иной характер. Соответствующие обязанности также установлены в ст. 5 DMA и включают в себя следующие ограничения:

- недопустимость включения в условия использования основной цифровой платформы ограничений для бизнес-пользователей на обращение за аналогичными услугами к другим участникам рынка, а также на

[248] Компания Meta признана в РФ экстремистской организацией и запрещена.

использование собственных прямых онлайн-площадок для реализации своих товаров и услуг конечным пользователям (в т.ч. по другим ценам);

- недопустимость установления для бизнес-пользователей запрета на использование промежуточного или дополнительного программного обеспечения, предоставляющего конечным пользователям возможность получать доступ или иным образом использовать цифровой контент, функции или иные элементы основной цифровой платформы;

- недопустимость установления запретов на бесплатное продвижение на основной цифровой платформе товаров и услуг бизнес-пользователей без использования специальных маркетинговых сервисов цифрового привратника;

- обязанность ежедневно по запросу рекламодателей или иных пользователей, которым предоставляются рекламные услуги, направлять им полную информацию о конечной стоимости оказанных рекламных услуг, а также о способах определения стоимости таких услуг.

В целом обязанности цифровых привратников по отношению к бизнес-пользователям сводятся к установлению свободного (не исключительного, не эксклюзивного) сотрудничества бизнес-пользователей с конкретным поставщиком услуг основной цифровой платформы, а также предполагают установление прозрачных правил рекламирования товаров и услуг на основной цифровой платформе.

Впрочем, помимо отмеченных выше запретов и ограничений, DMA также предусматривает возложение на цифровых привратников дополнительных обязанностей по отношению одновременно к конечным пользователям и к бизнес-пользователям. Соответствующие обязанности включают в себя:

- запрет на включение в условия предоставления услуг основной цифровой платформы требования об обязательном использовании

конкретных цифровых сервисов (идентификационных, браузерных, платежных, технических и др.);

- запрет на установление в качестве одного из условий использования основной цифровой платформы требования об обязательной подписке или регистрации в других цифровых сервисах данной платформы.

Данные обязанности в большей степени затрагивают уже интересы рынка в целом и направлены на предотвращение рисков монополизации отдельных рынков цифровых услуг со стороны крупных цифровых привратников. Однако более детально антимонопольные требования к осуществлению деятельности цифровыми привратниками закрепляются в ст. 6 DMA и включают в себя:

- недопустимость использования в конкуренции с бизнес-пользователями предоставленных цифровому привратнику или сгенерированных им данных в рамках предоставления услуг основной цифровой платформы соответствующим бизнес-пользователям;

- недопустимость установления ограничений (включая аппаратные и программные ограничения) на удаление дополнительных приложений, установленных в операционной системе цифрового привратника, но не являющихся необходимыми для ее нормального функционирования;

- недопустимость дискриминации программного обеспечения, разработанного третьими лицами, а также введения иных ограничений при установке и использовании ПО в рамках основной цифровой платформы;

- обязанность обеспечивать справедливые, разумные и недискриминационные условия для доступа к основной цифровой платформе и ее отдельным цифровым сервисам;

- обязанность создавать технические возможности для установки и использования программного обеспечения, разработанного третьими лицами (кроме программного обеспечения, несущего в себе риски для нормального функционирования аппаратного обеспечения и операционной системы);

- обязанность обеспечивать функциональную совместимость основной цифровой платформы с аппаратным и программным обеспечением.

В целом антимонопольные требования к цифровым привратникам предусматривают недопустимость использования данных бизнес-пользователей в конкуренции с ними, а также необходимость обеспечения свободного использования стороннего программного обеспечения на основной цифровой платформе.

При этом стоит отметить, что в ст. 7 DMA установлены дополнительные (специальные) антимонопольные требования к цифровым привратникам, которые предоставляют услуги цифровой онлайн-связи. В наиболее общем виде, они сводятся к обязанности соответствующих цифровых привратников обеспечить возможность свободной коммуникации (в текстовом, голосовом, групповом, аудио- и видео- форматах) между своими конечными пользователями и конечными пользователями других цифровых привратников. Соответствующие обязанности являются специальными и распространяются только на конкретную деятельность цифровых привратников.

Кроме того, следует отметить, что DMA также предусматривает возложение на цифровых привратников общих обязанностей в сфере предоставления ежегодной отчетности об исполнении положений DMA. Соответствующая отчетность (согласно ст. 11 DMA) должна направляться в Еврокомиссию и должна содержать в себе результаты аудита порядка обращения персональных данных в рамках основных цифровых платформы (данная отчетность через Еврокомиссию направляется в Европейский совет по защите данных), а также результаты обязательного к проведению внутрикорпоративного комплаенса соответствия деятельности цифровых привратников положениям DMA.

Что примечательно, отчетность цифровых привратников об исполнении требований DMA не носит конфиденциального характера.

Еврокомиссия после получения соответствующей отчетности размещает ее в открытом доступе на своем сайте, вследствие чего любой желающий может ознакомиться с результатами деятельности цифровых привратников по выполнению обязанностей, предусмотренных DMA. Как следствие, в дополнение к институциональному контролю со стороны Еврокомиссии в отношении цифровых привратников также косвенно применяется и общественный контроль[249].

Таким образом, все требования к цифровым привратникам, установленные Регламентом о цифровых рынках (DMA), могут быть подразделены на четыре группы:

1) обязанности цифровых привратников в части их взаимодействия с конечными пользователями (преимущественно связаны с обработкой и использованием их персональных данных);

2) обязанности цифровых привратников по отношению к бизнес-пользователям (преимущественно сводятся к установлению свободного сотрудничества бизнес-пользователей с конкретным поставщиком услуг основной цифровой платформы, а также предполагают установление прозрачных правил рекламирования товаров и услуг на основной цифровой платформе);

3) антимонопольные требования к цифровым привратникам (предусматривают недопустимость недобросовестной конкуренции, предотвращение рисков монополизации отдельных рынков цифровых услуг со стороны крупных цифровых привратников; необходимость обеспечения свободного использования стороннего программного обеспечения на основной цифровой платформе);

4) обязанности в сфере ежегодной отчетности о порядке обращения с персональными данными и о выполнении требований DMA.

---

[249] Schöning F., von Schreitter F. Showcases and showstoppers: the DMA’s impact on merger control in digital markets // Competition Law & Policy Debate. 2022. № 7(3). P. 121-129.

2.3.3. Наднациональное регулирование ИИ и криптоактивов в ЕС

Помимо наднационального регулирования цифровых услуг и цифровых рынков, содержащегося в DSA и DMA, в контексте принятия по предложению Комиссии Регламента об искусственном интеллекте (AIA) и Регламента о рынках криптоактивов (MiCA) к наднациональному регулированию цифровых рынков и цифровых услуг в ЕС также следует отнести наднациональное регулирование ИИ-систем и наднациональное регулирование криптоактивов в ЕС.

Регламент об искусственном интеллекте (AIA) в рамках своей ключевой цели направлен на формирование единого рынка законных, безопасных и заслуживающих доверия систем искусственного интеллекта, которые разрабатываются и применяются в строгом соответствии с положениями наднациональных актов ЕС о персональных данных, а также о правах человека в целом. Как отмечается в самом Регламенте, его положения находятся в полном соответствии с Хартией основных прав ЕС[250], требованиями в сфере недискриминации и гендерного равенства, Общим регламентом по защите данных (GDPR), Директивой о защите прав физических лиц при обработке персональных данных компетентными органами[251], конкурентным правом ЕС, наднациональными требованиями в сфере защиты прав потребителей и т.д.

При этом на основе AIA планируется обеспечить формирование именно единого рынка ИИ-систем в ЕС, устранив существовавшую ранее фрагментарность регулирования искусственного интеллекта на уровне отдельных национальных правопорядков государств – членов ЕС. В рамках единого рынка ИИ планируется осуществить формирование такого правого

[250] Charter of Fundamental Rights of the European Union // OJ C 326, 26.10.2012, p. 391–407.
[251] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA // OJ L 119, 4.5.2016, p. 89–131.

режима наднационального регулирования, при котором в масштабах всего Союза будет возможно свободное беспрепятственное распространение продуктов и услуг, связанных с технологиями искусственного интеллекта.

Если же говорить непосредственно о правовом режиме ИИ-систем, внедрение которого на уровне ЕС было осуществлено с принятием Регламента об искусственном интеллекте, то он опирается на риск-ориентированный подход, концентрируясь на создании строгих требований к разработке, поставке и использованию преимущественно ИИ-систем высокого риска (англ. high-risk AI systems).

К подобным ИИ-системам высокого риска, в частности, отнесены системы искусственного интеллекта, которые применяются напрямую или опосредовано в таких областях, как биометрическая идентификация лиц; управление и эксплуатация критической инфраструктуры; образование и профессиональная подготовка; осуществление трудовой деятельности и управление ею; предоставление государственных услуг; правоохранительная деятельность; управление миграцией и пограничный контроль; отправление правосудия и реализация демократических процедур (Приложение III к AIA). Кроме того, к ИИ-системам высокого риска также отнесены системы искусственного интеллекта, которые опосредованно или непосредственно применяются в отдельных сферах гармонизированного законодательства, включая законодательство о машинах, игрушках, гидроциклах, лифтах, системах защиты от взрывов, радиооборудовании и в иных сферах, указанных в Приложении II к AIA.

ИИ-системы высокого риска в обязательном порядке должны проходить контроль рисков и подпадать под действие специальных систем управления рисками. Также обучение ИИ-систем должно осуществляться на основе данных, соответствующих особым требованиям качества (в частности, такие данные не должны носить дискриминационного характера). ИИ-системы также должны быть «прозрачными» для пользователей и

должны соответствовать требованиям точности, надежности и кибербезопасности. Отдельно устанавливаются и требования к осуществлению надзора над ИИ-системами высокого риска со стороны человека. Кроме того, в AIA закрепляются ключевые обязанности поставщиков и пользователей ИИ-систем высокого риска. Предусматривается и закрепление специальных стандартов соответствия, сертификации и регистрации ИИ-систем.

Также AIA закрепляет перечень запрещенных практик, связанных с использованием ИИ-систем. Так, в частности, в соответствии с данным регламентом не допускается использование ИИ-систем в целях оказания целенаправленного воздействия на сознание, которое может повлечь за собой причинение физического или психологического вреда лицу – объекту воздействия или третьим лицам; в целях воздействия на поведение уязвимых групп лиц (детей, лиц старшего возраста и лиц с нарушениями интеллектуальных функций), которое может повлечь за собой причинение физического или психологического вреда; в целях оценки благонадежности поведения определенных групп лиц со стороны органов государственной власти (или от их имени), если такая оценка влечет за собой дискриминацию или создание неблагоприятных условий для соответствующих групп лиц; в целях удаленной биометрической идентификации лиц в режиме реального времени в общедоступных местах (за исключением случаев, когда такая идентификация осуществляется для поиска конкретных потерпевших от преступлений, для предотвращения конкретной, непосредственной и существенной угрозы жизни и физической безопасности, для поиска лиц, совершивших преступление или подозреваемых в совершении преступлений, наказание за которые составляет более трех лет лишения свободы).

При этом (в духе DSA и DMA) действию Регламента об искусственном интеллекте придан экстерриториальный характер, распространяющий сферу его применения не только на поставщиков (провайдеров) и пользователей

ИИ-систем, являющихся резидентами (гражданами) Европейского союза, но и на поставщиков и пользователей ИИ-систем из третьих стран, если соответствующие ИИ-системы распространяются на едином рынке искусственного интеллекта Европейского союза или используются на территории ЕС.

Несмотря на то, что AIA встретил определенную критику (прежде всего, в контексте защиты фундаментальных прав человека и гражданина, а также в сфере оборота персональных данных), он все же был принят. Принятие AIA позволит ЕС не только прямо расширить наднациональную компетенцию, сформировав единый рынок ИИ, но и создать продвинутый эффективный правовой режим регулирования ИИ, которого сейчас нет ни в одном государстве мира (преимущественно регулирование ИИ осуществляется через призму защиты персональных данных).

Что же касается наднационального регулирования криптоактивов на уровне наднационального законодательства ЕС, то здесь планы Комиссии не менее амбициозны.

Несмотря на то, что в соответствии с действующим наднациональным регулированием отдельные виды криптоактивов подпадают под действие требований ЕС, применение положений традиционного права к данным объектам является затруднительным. Кроме того, сегодня криптоактивы преимущественно регулируются в соответствии с наднациональными требованиями в сфере борьбы с отмыванием денежных средств и финансированием терроризма, но при этом не подпадают под действие актов о финансовых услугах, о защите прав потребителей и инвесторов (хотя порождают соответствующие риски)[252].

В соответствии с Регламентом о рынках криптоактивов (MiCA) обеспечивается формирование всеобъемлющего коммунитарного подхода к правовой квалификации и правовому регулированию криптоактивов и

[252] Advice on ‘Initial Coin Offerings and Crypto-Assets. ESMA. 2019; EBA report with advice on crypto-assets, 2019.

токенизированных традиционных финансовых активов на уровне ЕС. При этом изменения соответствующего наднационального регулирования нашли свое отражение не только на уровне специального Регламента MiCA, но и на уровне Директивы о рынках финансовых инструментов[253] (MiFID II) в части расширения традиционного определения финансовых инструментов. Также был запущен пилотный проект в сфере формирования специальной рыночной инфраструктуры, основанной на технологиях распределенного реестра[254].

Таким образом, на уровне ЕС в соответствующей сфере создано исчерпывающее регулирование криптоактивов на уровне ЕС, а также особая рыночная инфраструктура, пригодная для их обращения.

Для этого в соответствии с MiCA устанавливаются единые правила в таких сферах, как 1) требования к прозрачности и раскрытию информации при эмиссии криптоактивов и их допуске к организованным торгам; 2) требования об обязательной авторизации поставщиков услуг, связанных с криптоактивами, и эмитентом криптоактивов; 3) требования в сфере надзора над лицами, оказывающими услуги, связанные с криптоактивами, и эмитентами криптоактивов; 4) требования в сфере организации, функционирования и управления эмитентами криптоактивов и поставщиками услуг, связанных с криптоактивами; 5) требования в сфере защиты прав потребителей при эмиссии, торговле, обмене и хранении криптоактивов; 6) правила предотвращения злоупотреблений на рынке криптоактивов, ориентированные на сохранение целостности соответствующих рынков в рамках ЕС.

При этом сам режим правового регулирования криптоактивов (в соответствии с положениями MiCA) носит дифференцированный характер и

---

[253] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) // OJ L 173, 12.6.2014, p. 349–496.

[254] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (PE/88/2021/REV/2) // OJ L 151, 2.6.2022, p. 1–33.

предполагает установление различных требований к токенам, обеспеченным активами; токенам электронных денег; и иным криптоактивам, не относящимся к первым двум категориям.

Действие MiCA (уже традиционно) носит экстерриториальный характер и распространяется на любых лиц, которые эмитируют криптоактивы или предоставляют услуги, связанные с криптоактивами, на территории ЕС. Таким образом, под требования нового регламента фактически подпадают все участники мировой криптоиндустрии, поскольку их услуги оказываются в сети Интернет, в том числе действующей на территории ЕС.

В то же время из-под действия MiCA прямо исключен ряд субъектов и объектов, которые регулируются наднациональными актами ЕС в других сферах. В частности, требованиям MiCA не должны соответствовать финансовые инструменты (как они определены в MiFID II), электронные деньги (не токенизированные и подчиняющиеся требованиям Директивы об электронных деньгах[255]), депозиты (как они определены в Директиве о депозитах[256]), структурированные депозиты (в рамках MiFID II), инструменты секьюритизации[257]. Также MiCA не распространяется на Европейский центральный банк, Европейский инвестиционный банк; Европейский фонд финансовой стабильности, Европейский механизм стабильности, общественные международные организации, страховые компании, арбитражных управляющих. Кроме того, MiCA не действует и в отношении компаний, которые оказывают услуги, связанные с

[255] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC // OJ L 267, 10.10.2009, p. 7–17.

[256] Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes (recast) // OJ L 173, 12.6.2014, p. 149–178.

[257] Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012 // OJ L 347, 28.12.2017, p. 35–80.

криптоактивами, в рамках внутренней структуры одного холдинга (своим материнским компаниям или другим дочерним компаниям, входящим в состав холдинга).

Причины подобного ограничения сферы действия MiCA состоят в том, что все отмеченные выше группы общественных отношений регулируются специальным законодательством, а MiCA по отношению к ним будет выступать в качестве общего закона о криптоактивах в целом. Таким образом, в данном случае на уровне ЕС было принято решение прямо закрепить конкретные направления принципа *lex specialis derogat generali* в отношении положений MiCA.

В целом на основе MiCA планируется сформировать на уровне ЕС высокодифференцированный подход к регулированию криптоактивов, который не только будет учитывать отличие данного объекта прав от традиционных финансовых инструментов, но и будет принимать во внимание различную правовую природу самих криптоактивов (которые отличаются большим разнообразием).

В 2022 г. на уровне ЕС специальным образом был урегулирован единый рынок цифровых услуг, а также были сформированы единые требования о конкурентных и справедливых рынках в цифровом секторе. Данный шаг ознаменовал собой существенное расширение правового регулирования соответствующих рынков на уровне ЕС, которое до 2022 г. осуществлялось в соответствии с национальными законодательствами государств-членов.

При этом в рамках ключевых для этой сферы Регламента о едином рынке цифровых услуг и Регламента о конкурентных и справедливых рынках в цифровом секторе были сформированы современные эффективные правила, обеспечивающие 1) защиту авторских прав и интеллектуальной собственности в цифровой среде с учетом актуальных вызовов цифровой эпохи; 2) адекватное цифровой сфере антимонопольное регулирование,

учитывающее, в том числе, современные вызовы для цифрового суверенитета ЕС и ведения IT-деятельности субъектами малого и среднего предпринимательства в ЕС; 3) свободное движение цифровых услуг на едином рынке ЕС (включая посреднические услуги по передаче, хранению, распределению или размещению информации в сети Интернет).

Также в 2023 г. был принят Регламент о рынках криптоактивов, призванный обеспечить всеобъемлющее правового регулирование криптоактивов (с учетом как их внутренней дифференциации, так и их внешнего отграничения от традиционных финансовых инструментов).

В дополнение к отмеченным регламентам сегодня на уровне ЕС проходят процедуры принятия Регламент об искусственном интеллекте. В соответствии с данным регламентом на уровне ЕС планируется внедрить коммунитарные требования к созданию, реализации и пользованию системами ИИ.

Глава III. Проблемы и перспективы регулирования цифрового пространства на уровне ЕАЭС

§ 3.1. Особенности и основные направления регулирования цифрового пространства в рамках ЕАЭС

Необходимость развития цифрового направления интеграции в рамках ЕАЭС была зафиксирована еще в 2016 г. в рамках Цифровой повестки ЕАЭС[258] (спустя два года после подписания Договора о ЕАЭС[259]). Кроме того, в декабре 2020 г. создание цифрового пространства ЕАЭС было прямо отнесено к основным стратегическим направлениям развития евразийской интеграции[260]. В 2023 г. цифровая повестка стала приоритетным направлением председательства России в высших органах ЕАЭС[261].

Таким образом, вопросы наднационального регулирования цифрового пространства являются достаточно актуальными для ЕАЭС на протяжении всего периода существования данного интеграционного объединения. Как отмечает К.А. Ермак, «несмотря на то, что развитие интеграции в информационной сфере напрямую не закреплено в Договоре о ЕАЭС, данное направление имеет статус самостоятельного вектора евразийской интеграции»[262].

Тем не менее, правовое регулирование цифрового пространства в ЕАЭС в настоящее время находится на этапе своего становления. В отличие

---

[258] Заявление о цифровой повестке ЕАЭС (подписано главами государств-членов ЕАЭС 26 декабря 2016 г.). [Электронный ресурс] // Режим доступа: https://eec.eaeunion.org/upload/medialibrary/d9c/Proekt-Zayavleniya_na-podpisanii.pdf (дата обращения: 31.01.2024).

[259] Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014) // Официальный сайт Евразийской экономической комиссии http://www.eurasiancommission.org/, 05.06.2014.

[260] Решение Высшего совета ЕАЭС от 11.12.2021 № 12 «О стратегических планах развития евразийской экономической интеграции» (документ опубликован не был) // СПС «КонсультантПлюс»

[261] Лю К.А. Основные направления международно-правового и наднационального регулирования цифрового пространства в рамках ЕАЭС на современном этапе // Право и управление. XXI век. 2024. Т. 20. № 1. С. 84-91.

[262] Ермак К.А. Информационная безопасность как элемент интеграции в рамках ЕАЭС // Социальные новации и социальные науки. 2023. №3 (12). С. 132-142.

от ЕС, в рамках евразийской интеграции направления соответствующего наднационального регулирования существенно сужены и не охватывают собой достаточно широкого перечня значимых областей[263].

Можно предположить, что подобная ситуация обусловлена отсутствием положений о цифровом пространстве, основ его наднационального регулирования в Договоре о ЕАЭС. Подписанный в 2014 г. учредительный договор ЕАЭС не предусматривал решения вопросов, связанных с углубляющейся цифровизацией всех сфер общественных отношений. Договор о ЕАЭС весьма узко подошел к регулированию цифровой сферы, ограничившись закреплением основ информационного взаимодействия между органами публичной власти государств-членов в виде единой информационной системы[264].

Несмотря на то, что направления интеграции в цифровой сфере были существенно расширены в рамках Цифровой повестки ЕАЭС уже в 2016 г., положения Договора о ЕАЭС напрямую дополнены не были. Поэтому такое направление интеграции, как построение единого цифрового пространства (включая формирование общих цифровых рынков, общих рынков цифровых услуг, общего регулирования криптоактивов и т.п.) в учредительном договоре ЕАЭС не закреплено[265].

По мнению И.М. Поповой, отмеченные ограничения несколько осложняют развитие и реализацию цифровых аспектов евразийской интеграции, поскольку в отсутствие основополагающих положений Договора о ЕАЭС дополнительную сложность приобретает разграничение компетенций между институтами ЕАЭС, а также определение источников финансирования проектов и программ в рамках развития цифрового

[263] Лю К.А. Указ. соч. С. 85.
[264] Там же.
[265] Там же.

направления интеграции[266]. Внесение соответствующих дополнений в Договор о ЕАЭС не обсуждается и в настоящее время.

Если обратиться к опыту ЕС в аналогичной сфере, то можно заметить, что и учредительные договоры ЕС равным образом не предусматривали напрямую возможность расширения интеграции на цифровую сферу. Наднациональное европейское регулирование всех вопросов построения единого цифрового пространства строилось вторичным законодательством с опорой на предоставленную ЕС и его институтам компетенцию в соответствии с принципом наделения полномочиями (англ. principle of conferral)[267]. При этом различные аспекты цифровой интеграции в рамках ЕС были реализованы с опорой не только на исключительную компетенцию ЕС (ст. 3 ДФЕС), но и на совместную компетенцию ЕС и государств-членов (ст. 4 ДФЕС), а также на координационную и дополняющую компетенцию ЕС (ст. 6 ДФЕС).

Так, например, непосредственной правовой основой для принятия DMA и DSA выступили положения ст. 114 ДФЕС, в соответствии с которой ЕС в рамках совместной компетенции с государствами-членами может принимать акты, обеспечивающие сближение национального законодательства государств-членов в целях обеспечения эффективного функционирования единого рынка.

Таким образом, сам факт отсутствия положений об интеграции в цифровой сфере в рамках учредительных договоров интеграционных объединений не является серьезным препятствием для формирования новых направлений наднационального регулирования цифрового пространства[268].

---

[266] Попова И.М. Проблемы реализации цифровой повестки ЕАЭС // Вестник международных организаций: образование, наука, новая экономика. 2021. №1. С. 127-141.
[267] Европейское право. Отрасли права Европейского Союза и Евразийского экономического союза: учебник / рук. авт. кол. и отв. ред. Л.М. Энтин, М.Л. Энтин. М.: ИНФРА-М, 2023. 416 с.
[268] Лю К.А. Указ. соч. С. 86.

Представляется, что сдерживающим цифровую интеграцию фактором в рамках ЕАЭС, скорее, выступает неравномерность развития государств – членов ЕАЭС как непосредственно в цифровой сфере, так и в части ее правового регулирования. В настоящее время в государствах – членах ЕАЭС наблюдаются различные уровни доступа к цифровым услугам, масштабы их развитости и внедренности в общественную жизнь и государственное управление, а также разная степень проработанности правового регулирования цифровой сферы[269]. Так, сегодня не во всех государствах-членах ЕАЭС существует достаточное регулирование порядка обращения персональных данных, предоставления цифровых услуг.

При этом отмеченная разница в страновых подходах к регулированию цифрового пространства не может быть эффективно преодолена на наднациональном уровне ввиду действия принципа главенства суверенитета[270]. Данный принцип применяется, в том числе, в рамках попыток сформировать общее цифровое пространство ЕАЭС. Как прямо отметил Министр ЕЭК К. Минасян, институты ЕАЭС стремятся создать институционально-правовую инфраструктуру, основанную, прежде всего, на национальном суверенитете, а построение общего цифрового пространства ЕАЭС должно осуществляться не в виде единой платформы, а в виде распределенной сети[271].

На практике принцип главенства суверенитета означает, что все ключевые акты и стратегические документы, обеспечивающие формирование общего цифрового пространства в рамках ЕАЭС, подчиняются, в первую очередь, национальным интересам государств – членов ЕАЭС и национальным стратегиям в соответствующей сфере. Непосредственно же на

---

[269] Лю К.А. Указ. соч. С. 86.
[270] Там же.
[271] Министр ЕЭК Карине Минасян в интервью CNews – об общих цифровых экосистемах Армении, Белоруссии, Казахстана, Кыргызстана и России // ЕЭК: официальный сайт. [Электронный ресурс]. Режим доступа: https://eec.eaeunion.org/news/speech/15-01-2020-1/ (дата обращения: 31.01.2024).

наднациональном уровне могут осуществляться лишь шаги по координации действий государств-членов в цифровой сфере и по устранению барьеров на общих рынках ЕАЭС. При этом имплементация наднациональных положений осуществляется на уровне государств-членов, что предоставляет им дополнительную возможность для гибкой интеграции в цифровой сфере[272].

Иными словами, если в ЕС разработка и внедрение цифровой повестки осуществляется преимущественно на наднациональном уровне (по принципу «сверху-вниз»), то в рамках ЕАЭС выработка правовых и политических основ происходит в государствах-членах, после чего обеспечивается их координация и применение на интеграционном уровне (по принципу «снизу-вверх»)[273].

При этом соответствующий подход, как правило, напрямую противопоставляется подходу ЕС. Принцип главенства суверенитета и организации интеграционных процессов «снизу-вверх» расценивается как конкурентное преимущество евразийской модели интеграции, которое может способствовать ее восприятию по всему миру (в рамках иных интеграционных объединений)[274].

Выбранный в рамках ЕАЭС подход действительно не лишен ряда преимуществ. Определение приоритетов развития интеграции на национальном уровне (а не на наднациональном) способствует как преимущественному учету всех государств-членов, так и большей устойчивости интеграции в целом. Принцип главенства суверенитета обеспечивает и более полный учет национальных особенностей в рамках выработки и реализации наднациональных интеграционных инициатив и проектов[275]. Параллельно принятие ключевых решений на уровне глав

---

[272] Лю К.А. Указ. соч. С. 86.
[273] Там же.
[274] См., например: Саркисян Т.С. Интеграционный "План ГОЭЛРО" для XXI века // Россия в глобальной политике. 2021. №3 (109). С. 136-149.
[275] Лю К.А. Указ. соч. С. 87.

государств-членов в общих интересах всех участников интеграции содействует реализации наднациональных инициатив, подкрепленных политической волей руководителей стран-участниц[276].

Однако отмеченному подходу свойственны и определенные недостатки. Необходимость согласования всех наднациональных инициатив с существующими правовыми актами и стратегическими документами государств-членов с последующим утверждением соответствующих инициатив на высшем политическом уровне обусловливает более медленные темпы развития и углубления интеграции (в т.ч. в цифровой сфере). Кроме того, перенос фокуса внимания на национальный уровень существенно снижает значимость и политическое влияние интеграционных институтов. В силу главенства суверенитета наднациональные акты лишь в ограниченном объеме могут определять основы для развития интеграции (за исключением Договора о ЕАЭС). Наднациональные акты либо определяют направления развития в общем концептуальном виде, либо, напротив, касаются регулирования отдельных деталей[277].

Все это способствует более медленному внедрению новых направлений наднационального регулирования цифрового пространства на уровне ЕАЭС.

Непосредственным следствием данной ситуация является то, что в настоящее время на уровне ЕАЭС отсутствует общее регулирование цифровых рынков (включая антимонопольное регулирование), цифровых услуг, искусственного интеллекта, криптоактивов и иных передовых сфер[278]. Кроме того, на уровне ЕАЭС не сформированы наднациональные правовые основы противодействия кибертерроризму и киберпреступности[279]. Лишь косвенно (и весьма фрагментарно) на уровне ЕАЭС закрепляются требования

---

[276] Попова И.М. Указ. соч. С. 133.
[277] Лю К.А. Указ. соч. С. 87.
[278] Там же.
[279] Бороздин А.Н., Коварда В.В. Анализ системы обеспечения защиты информации в процессе цифровизации ее оборота в рамках ЕАЭС в аспекте повышения экономической безопасности // Вестник Евразийской науки. 2020. Т. 12. № 4. С. 1-15.

к надежности и безопасности информационно-коммуникационной инфраструктуры[280]. Весьма ограничено регулируется на наднациональном уровне и порядок обращения персональных данных (преимущественно в рамках общих цифровых баз для поиска работы в государствах – членах ЕАЭС).

В современных условиях развития цифровых аспектов евразийской интеграции, как правило, речь идет о реализации цифровой повестки в сфере единого таможенного регулирования[281]. В практической плоскости именно для цифровизации таможенного регулирования свойственны наиболее активные процессы: введение цифровой системы таможенного администрирования[282] и электронного документооборота[283], создание цифровых транспортных коридоров[284], а также создание цифровой (электронной) таможни[285]. При этом в последние годы (с 2019 г.) актуальность набирает также наднациональное регулирование электронной торговли[286].

Стоит отметить и положения Договора о ЕАЭС, а также протоколов к нему, в рамках которых напрямую затрагиваются вопросы наднационального регулирования цифровой сферы. В частности, исходя из анализа соответствующих норм, можно сделать вывод о том, что в настоящее время в рамках правового пространства ЕАЭС особое внимание уделяется обороту

---

[280] Ермак К.А. Информационная безопасность как элемент интеграции в рамках ЕАЭС // Социальные новации и социальные науки. 2023. №3 (12). С. 132-142.
[281] Лю К.А. Указ. соч. С. 87.
[282] Иванова О.Б., Хапилин А.Ф., Хапилин С.А. Цифровая повестка ЕАЭС в контексте модернизации системы таможенного администрирования // Вестник Ростовского государственного экономического университета (РИНХ). 2020. № 1 (69). С. 157-163.
[283] Шаститко А.Е., Шпакова А.А. Регулирование трансграничного электронного документооборота в Евразийском экономическом союзе // Государственное управление. Электронный вестник. 2018. № 71. С. 242-269.
[284] Зуева А.М., Шайдуллова М.В. Цифровой транспортный коридор как новый элемент в организации таможенного контроля // NovaUm.Ru. 2018. № 13. С. 99–101.
[285] Мозер С.В., Секербаева Д.К. К вопросу о функционировании тематического блока «электронная таможня» в Евразийском экономическом союзе // Социально-политические науки. 2020. Т. 10. № 1. С. 49-59.
[286] Ревина С.Н., Лунева У.С. Вопросы таможенного регулирования в условиях развития интернет-торговли // МНИЖ. 2023. №4 (130). С. 1-5.

неперсональных государственных данных, а также закупкам для государственных нужд.

В соответствии с положениями Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза[287] устанавливаются общие основы формирования интегрированной информационной системы Союза. Основными задачами подобной интегрированной системы выступают обеспечение электронного документооборота между государствами, а также предоставление равного доступа к официальной информации государств-членов. Дополняют данные положения нормы Протокола о порядке формирования и распространения официальной статистической информации Евразийского экономического союза[288]. Во многом к данному направлению интеграции в цифровой сфере могут быть отнесены и проекты по цифровизации таможни и таможенного документооборота[289].

Отдельные аспекты цифровой интеграции можно встретить и в рамках Протокола о порядке регулирования закупок[290], которым устанавливаются общие правовые основы осуществление закупок в электронном формате, порядок деятельности электронных торговых площадок и операторов таких площадок.

Несмотря на отсутствие прямого указания на создание наднационального регулирования в цифровой сфере, определенное значение

---

[287] Приложение № 3 к Договору о Евразийском экономическом союзе. Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза // Официальный сайт Евразийской экономической комиссии http://www.eurasiancommission.org/, 05.06.2014.

[288] Приложение № 4 к Договору о Евразийском экономическом союзе. Протокол о порядке формирования и распространения официальной статистической информации Евразийского экономического союза // Официальный сайт Евразийской экономической комиссии http://www.eurasiancommission.org/, 05.06.2014.

[289] Лю К.А. Указ. соч. С. 88.

[290] Приложение № 25 к Договору о Евразийском экономическом союзе. Протокол о порядке регулирования закупок // Официальный сайт Евразийской экономической комиссии http://www.eurasiancommission.org/, 05.06.2014.

для цифровой интеграции в рамках ЕАЭС имеет Протокол об охране и защите прав на объекты интеллектуальной собственности[291].

Таким образом, в настоящее время можно говорить о существовании следующих основных направлений правового регулирования цифрового пространства на уровне ЕАЭС[292]:

1) наднациональное регулирование порядка обращения официальной государственной информации и иных неперсональных данных в пространстве ЕАЭС (сюда же можно отнести проекты в сфере цифровой таможни ЕАЭС);

2) наднациональное регулирование цифровых аспектов публичных закупок, осуществляемых на общих рынках ЕАЭС;

3) наднациональное регулирование в сфере защиты интеллектуальной собственности и авторских прав в пространстве ЕАЭС.

Наднациональное регулирование порядка обращения официальной государственной информации и иных неперсональных данных представляет собой единственное направление, которое было закреплено в Договоре о ЕАЭС. Соответствующим аспектам посвящен Раздел V Договора о ЕАЭС, которым предусматривается формирование интегрированной информационной системы ЕАЭС (ст. 23), а также устанавливаются общие принципы формирования и распространения официальной статистической информации (ст. 24).

Интегрированная информационная система ЕАЭС (ИИС ЕАЭС) представляет собой цифровое пространство, в рамках которого обеспечивается информационное взаимодействие между органами государственной власти государств-членов и институтами ЕАЭС. В рамках соответствующей системы интегрируются территориально распределенные информационные ресурсы государств – членов ЕАЭС и информационные

---

[291] Приложение № 26 к Договору о Евразийском экономическом союзе. Протокол об охране и защите прав на объекты интеллектуальной собственности // Официальный сайт Евразийской экономической комиссии http://www.eurasiancommission.org/, 05.06.2014.
[292] Лю К.А. Указ. соч. С. 90.

ресурсы Евразийской экономической комиссии (далее также — ЕЭК, Комиссия).

Сфера подобной интеграции ограничена сугубо информационным обеспечением общих процессов, реализуемых в рамках ЕАЭС. Предполагается формирование трансграничного пространства доверия (в т.ч. на основе использования современных информационных технологий). При этом в соответствии с ч. 3 ст. 23 Договора о ЕАЭС устанавливается, что в целях обеспечения информационного взаимодействия государства-члены проводят согласованную политику в области информатизации и информационных технологий.

Положения Раздела V Договора о ЕАЭС находят свою конкретизацию в рамках Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках ЕАЭС (далее также — Протокол № 3). Соответствующим протоколом закрепляются общие принципы информационного взаимодействия в рамках ЕАЭС, порядок создания и функционирования ИИС ЕАЭС, порядок сбора и распространения официальной статистической отчетности и другие базовые вопросы в сфере сбора и обращения неперсональных данных. Именно на обеспечение свободного и прозрачного межгосударственного обмена данными, в соответствии с Протоколом, направлено формирование трансграничного пространства доверия в рамках ЕАЭС.

При этом ИИС ЕАЭС, представляя собой непосредственную форму реализации трансграничного пространства доверия, включает в себя интегрированную информацию в таможенной сфере; в антимонопольной сфере; в сфере технического регулирования и стандартизации; в рамках валютной, финансовой, промышленной, энергетической политики, а также в сфере защиты интеллектуальной собственности и в ряде других направлений интеграции (ст. 3 Протокола № 3).

В частности, именно в рамках формирования трансграничного пространства доверия и функционирования ИИС ЕАЭС осуществляется цифровизация таможенной деятельности. Также можно отметить проект по созданию Евразийской сети промышленной кооперации, субконтрактации и трансфера технологий[293]. Ключевой целью данного проекта является формирование цифровой экосистемы для свободного взаимодействия субъектов промышленной деятельности (включая субъекты малого и среднего бизнеса) в пространстве ЕАЭС. Предполагается, что Евразийская сеть будет способствовать созданию новых производственных цепочек, развитию инноваций, продвижению продукции национальных производителей на общих рынках ЕАЭС.

Впрочем, в рамках создания трансграничного пространства доверия также реализуются и проекты в иных сферах. В частности, в 2021 г. была запущена Унифицированная система поиска «Работа без границ»[294], призванная стать цифровой базой для интеграции в трудовой сфере. Внедрение соответствующей системы способствовало повышению мобильности рабочей силы, расширению географии поиска работы или работников и, в целом, стало важным для обеспечения свободы передвижения рабочей силы в цифровую эпоху.

В наиболее общем виде все отмеченные аспекты оказываются связаны с оборотом цифровых неперсональных данных (государственной статистики, данных о транзите товаров, данных о грузоперевозках, данных о состоянии рынка труда, вакансиях и др.) в пространстве ЕАЭС. Это направление в настоящее время является перспективным для развития, поскольку оно в

---

[293] Решение Евразийского межправительственного совета от 30 апреля 2019 года № 2 «О реализации проекта "Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий"» // Официальный сайт Евразийского экономического союза www.eaeunion.org, 06.05.2019.

[294] Проект «Работа без границ» стартовал в ЕАЭС // ЕЭК: официальный сайт. 01.07.2021. [Электронный ресурс]. Режим доступа: https://eec.eaeunion.org/news/proekt-rabota-bez-granic-startoval-v-eaes/ (дата обращения: 01.02.2024).

полной мере соответствует основным экономическим целям евразийской интеграции.

В то же время, несмотря на наличие непосредственной связи с цифровой сферой, внедрение трансграничного пространства доверия и ИИС ЕАЭС направлено, в первую очередь, на повышение эффективности межгосударственного обмена информацией в сфере свободного передвижения традиционных (а не цифровых) товаров, работ и капиталов, а также в сфере публичного управления и обмена статистической информацией. Об этом же свидетельствуют и задачи, поставленные ЕЭК в рамках формирования ИИС ЕАЭС 3.0 до 2025 г.[295]

Наличие подобной тесной связи не позволяет рассматривать соответствующее направление как значительный шаг на пути к построению единого цифрового пространства ЕАЭС. Обмен цифровыми неперсональными данными представляет собой важный начальный элемент для формирования общего цифрового пространства, однако в современных реалиях требуется гораздо более глубокая интеграция именно в цифровых сферах общественной жизни.

Наднациональное регулирование цифровых аспектов публичных закупок в ЕАЭС осуществляется в соответствии с положениями ст. 88 Договора о ЕАЭС, а также положениями Протокола о порядке регулирования закупок (далее также — Протокол № 25).

Компетенция в сфере правового регулирования публичных закупок полностью предоставлена государствам – членам ЕАЭС. Согласно абз. 1 ч. 1 ст. 88 Договора о ЕАЭС, прямо установлено, что регулирование государственных закупок осуществляется в соответствии с национальным законодательством и международными договорами государств – членов ЕАЭС. При этом положения Протокола № 25 не носят строго императивного

[295] Решение Коллегии Евразийской экономической комиссии от 06.09.2022 N 125 «О техническом задании на развитие интегрированной информационной системы Евразийского экономического союза» // Официальный сайт Евразийского экономического союза http://www.eaeunion.org/, 09.09.2022.

характера. Как указано в ст. 3 данного протокола, приведение национального законодательства в соответствие с наднациональными правилами в сфере закупок требуется только в том случае, если из положений законодательства государства-члена следует иной смысл, чем установлено Протоколом № 25.

В подобном контексте наднациональное регулирование государственных закупок на уровне ЕАЭС приобретает субсидиарный характер. Оно призвано обеспечить мягкую гармонизацию национальных подходов к осуществлению государственных закупок на общих рынках ЕАЭС.

В части наднационального регулирования непосредственно цифровых аспектов государственных закупок Договор о ЕАЭС и Протокол № 25 достаточно скупы. Так, в ст. 88 Договора о ЕАЭС в соответствующей сфере устанавливается лишь общий принцип информационной открытости и прозрачности закупок, а также принцип беспрепятственного доступа поставщиков из государств – членов ЕАЭС к участию в закупках, проводимых в электронном формате. Последний принцип обеспечивается взаимным признанием электронных цифровых подписей в государствах – членах ЕАЭС.

Впрочем, проведение закупок в электронном формате в соответствии с положениями Протокола № 25 представляет собой не обязательство государств – членов ЕАЭС, а их стремление. Ст. 4 Протокола № 25 говорит о том, что государства-члены обеспечивают проведение в электронном формате только конкурса и аукциона и должны стремиться перейти к электронному формату иных способов закупок. В ст. 28 Протокола № 25 закрепляется, что государства-члены стремятся перейти на электронный формат заключения контрактов о закупках к 2016 г. Таким образом, инициатива по внедрению электронных форматов закупок полностью принадлежит государствам – членам ЕАЭС.

Более детально сформулированы положения Протокола № 25 об обеспечении информационной открытости и прозрачности закупок. Так, в соответствии со ст. 29 данного протокола устанавливается, что каждое государство – член ЕАЭС создает специальный веб-портал, публикует на нем информацию о закупках, размещает реестр недобросовестных поставщиков, а также информацию о действующем национальном законодательстве в сфере закупок. Вся указанная информация размещается, в том числе, на русском языке. Доступ к информации свободный. Кроме того, государства-члены определяют ограниченный перечень электронных торговых площадок в качестве места доступа к информации о закупках и об электронных услугах в соответствующей сфере.

В целом, как можно заметить, в рамках наднационального регулирования цифровых аспектов публичных закупок ЕАЭС также находится на начальном этапе. На интеграционном уровне сегодня заложены лишь общие основы организации закупочной деятельности в электронном формате. Общие системы документооборота, интегрированные цифровые системы, а равно единые цифровые документы (за исключением цифровой подписи) не создаются. Как и в рамках оборота неперсональных данных в цифровом формате, здесь наднациональное регулирование концентрируется преимущественно на обеспечении свободного доступа к информации о закупках и их правовом регулировании в государствах – членах ЕАЭС.

Наднациональное регулирование в сфере защиты интеллектуальной собственности и авторских прав в цифровом пространстве ЕАЭС основано на положениях Раздела XXIII Договора о ЕАЭС, а также на Протоколе об охране и защите прав на объекты интеллектуальной собственности (далее также — Протокол № 26).

В целом положения учредительного договора и Протокола № 26 концентрируются на традиционных (не цифровых) аспектах защиты интеллектуальной собственности. При этом перед интеграционным

объединением здесь ставится две ключевые задачи: гармонизация законодательства государств – членов ЕАЭС в сфере охраны и защиты интеллектуальной собственности, а также непосредственная защита интересов обладателей прав на объекты интеллектуальной собственности (ч. 1 ст. 89 Договора о ЕАЭС).

Тем не менее в качестве одного из направлений интеграционного сотрудничества прямо названа защита прав на объекты интеллектуальной собственности, в том числе в сети Интернет (п. 5 ч. 2 ст. 89 Договора о ЕАЭС).

В соответствии с положениями ст. 2 Протокола № 26 программы для ЭВМ прямо отнесены к объектам интеллектуальной собственности. Согласно абз. 2 ст. 9 Протокола № 26, охрана программ для ЭВМ осуществляется в соответствии с правовым режимом, установленным для охраны литературных произведений в Бернской конвенции об охране литературных и художественных произведений[296]. Также предусмотрена охрана прав интеллектуальной собственности на топологию интегральных микросхем (Раздел XI Протокола № 26).

Указанные категории объектов интеллектуальной собственности действительно относятся к цифровому пространству (поскольку предназначены для использования в качестве компьютерного обеспечения или в качестве основы для функционирования информационно-коммуникационной инфраструктуры).

Однако современный уровень распространенности информационно-коммуникационных технологий ставит перед правовым регулированием (в том числе и наднациональным) гораздо большее количество вызовов, которые в действующем наднациональном регулировании ЕАЭС не находят своего отражения. Несмотря на то, что ст. 89 Договора о ЕАЭС было прямо

---

[296] Бернская Конвенция по охране литературных и художественных произведений от 09.09.1886 (ред. от 28.09.1979) // Бюллетень международных договоров. 2003. №9.

указано на защиту интеллектуальной собственности в сети Интернет, соответствующее направление интеграции все еще не сформировано.

При этом потребность в актуализации наднационального регулирования цифрового пространства в целом хорошо осознается в рамках ЕАЭС. Вызовы современной цифровой эпохи порождают необходимость в расширении ключевых направлений соответствующего регулирования как в целях обеспечения устойчивого развития частного цифрового сектора, так и в целях укрепления цифрового суверенитета государств – членов ЕАЭС и всего интеграционного объединения.

§ 3.2. Направления стратегического развития наднационального регулирования цифрового пространства в рамках ЕАЭС

Актуальные концептуальные основы стратегического развития наднационального регулирования цифрового пространства в рамках ЕАЭС нашли свое закрепление в Цифровой повестке ЕАЭС 2016 г. Она представляет собой общий концептуальный документ стратегического планирования, в котором закреплены ключевые цели, задачи и направления развития цифрового аспекта евразийской интеграции.

В наиболее общем виде необходимость разработки и реализации цифровой повестки ЕАЭС была обусловлена стремлением повысить конкурентоспособность ЕАЭС и государств – членов ЕАЭС в цифровой сфере. Платформа ЕАЭС предоставляет дополнительные возможности для планирования и реализации масштабных цифровых инициатив в рамках общих рынков интеграционного объединения[297].

Особенно актуальной опора на наднациональную платформу становится в условиях масштабных антироссийских санкций[298],

[297] Саркисян Т.С. Интеграционный "План ГОЭЛРО" для XXI века // Россия в глобальной политике. 2021. №3 (109). С. 136-149.

[298] Мишустин назвал Россию «чемпионом мира» по числу введенных против нее санкций // ТАСС. 15 марта 2023 г. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/17274023 (дата обращения: 03.02.2024).

ограничивающих доступ отечественных организаций к зарубежным инновационным технологиям и решениям[299]. Реимпорт и реэкспорт высоких технологий через таможенную территорию ЕАЭС активно используется уже сейчас[300], однако соответствующая деятельность носит «серый» характер (в том числе, ввиду отсутствия общего наднационального регулирования цифровых рынков, импорта высокотехнологичной продукции, оказания цифровых услуг и т.д.).

Ключевой целью Цифровой повестки является актуализация интеграционных механизмов сотрудничества с учетом вызовов цифровой эпохи для обеспечения устойчивого экономического роста государств – членов ЕАЭС. При этом обеспечить достижение данной цели планируется за счет синхронизации процессов цифровой трансформации и гармонизации правового регулирования цифровой сферы в государствах – членах ЕАЭС.

В основу достижения данной цели положен принцип главенства суверенитета государств – членов ЕАЭС, который предполагает, что формирование наднационального регулирования цифровой сферы не должно препятствовать свободному развитию цифровых рынков и цифрового права государств-членов. Национальные компетенции в соответствующих сферах должны быть лишь согласованы (гармонизированы) на наднациональном уровне в части, касающейся построения общих рынков и достижения иных экономических целей интеграции.

Таким образом, Цифровая повестка ЕАЭС продолжает общий тренд на формирование наднационального регулирования цифровой сферы по

---

[299] Британия оставит российский процессор без технологий // Lenta.ru. 5 мая 2022 г. [Электронный ресурс]. Режим доступа: https://lenta.ru/news/2022/05/05/buy/ (дата обращения: 03.02.2024); Какие микропроцессоры разрабатывают в России? И что с ними будет из-за санкций? // ТАСС. 10 июня 2022 г. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/14868777 (дата обращения: 03.02.2024).

[300] См., например: Кошелева О.Э., Воробьева М.Д. Параллельный импорт в качестве антисанкционной меры // Бюллетень информационных технологий. 2023. №1 (25). С. 39-44; Сонин В.В. Легальность параллельного экспорта товаров с зарегистрированными товарными знаками из КНР в Россию в современных условиях (анализ китайского законодательства и судебной практики). М., 2023. 10 с.

принципу «снизу-вверх». Концептуальных изменений, которые позволили бы форсировать развитие евразийской интеграции в цифровой сфере, Цифровая повестка не предусматривает.

Конкретизация положений Цифровой повестки ЕАЭС была осуществлена на уровне Основных направлений реализации цифровой повестки ЕАЭС до 2025 г.[301]

Основные направления представляют собой политический документ общего характера. В них находят свое закрепление лишь наиболее общие принципы и направления развития цифровых аспектов евразийской интеграции. Так, в частности, приоритетными направлениями названы: содействие цифровой трансформации экономики и кросс-отраслевой трансформации; цифровизация процессов управления и интеграционных процессов; цифровая трансформация рынков товаров, услуг, капитала и рабочей силы; развитие цифровой инфраструктуры и обеспечение защищенности цифровых процессов.

Как можно заметить, положения Основных направлений реализации цифровой повестки ЕАЭС ориентируются преимущественно на применение цифровых средств к традиционным сферам евразийской интеграции. Они предполагают сотрудничество в сфере цифровизации традиционных отраслей экономики и управления (в том числе наднационального), но не в сфере построения наднациональных основ регулирования новых цифровых отраслей (рынков больших данных, машинного обучения, искусственного интеллекта, криптоактивов и др.).

Единственным направлением, которое непосредственно связано с построением новой цифровой среды, является обеспечение стабильного функционирования и безопасности цифровой инфраструктуры. Однако и

---

[301] Решение Высшего Евразийского экономического совета от 11.10.2017 N 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» // Официальный сайт Евразийского экономического союза http://www.eaeunion.org/, 10.11.2017.

данный аспект в рамках Основных направлений реализации цифровой повестки понимается достаточно узко.

В целом Цифровая повестка ЕАЭС и Основные направления ее реализации не содержат в себе положений, направленных на обеспечение прорывных решений в сфере построения новой парадигмы наднационального регулирования цифрового пространства. Соответствующие акты стратегического планирования лишь ограниченно расширяют компетенции ЕАЭС в части развития цифровых аспектов интеграции (на базе уже существующих направлений интеграционного взаимодействия).

Формирование новых аспектов наднационального регулирования цифрового пространства осуществляется точечно в рамках отдельных проектов или приоритетных направлений. Именно проектный подход выбран в качестве основного механизма реализации Цифровой повестки ЕАЭС[302]. В рамках соответствующего подхода вначале со всеми государствами-членами согласовываются определенные инициативы, после чего на их основе разрабатываются и утверждаются конкретные проекты.

Преимуществами проектного подхода в реализации Цифровой повестки ЕАЭС является высокая степень конкретизации задач и целевых показателей, достижение которых должно быть осуществлено в максимально узкой сфере. Кроме того, в реализацию проектов вовлекаются все государства – члены ЕАЭС, что существенно повышает степень гармонизации их цифровых инициатив на наднациональном уровне. Таким образом, согласованные и запущенные проекты выступают в качестве весьма эффективного инструмента точечного развития цифровых аспектов евразийской интеграции[303].

---

[302] Решение Евразийского межправительственного совета от 01.02.2019 N 1 «О механизмах реализации проектов в рамках цифровой повестки Евразийского экономического союза» // Официальный сайт Евразийского экономического союза http://www.eaeunion.org/, 18.02.2019.

[303] Попова И.М. Указ. соч. С. 136.

Однако проектный подход по своему функционалу изначально ориентирован на реализацию отдельных, весьма узких, задач. Как следствие, в отсутствие проработанной концептуальной правовой базы, объединяющей все проекты в рамках достижения единых масштабных целей, применение проектного подхода влечет за собой низкую связанность реализуемых цифровых инициатив. Применение проектного подхода требует гораздо большей степени конкретизации целей и задач ЕАЭС на уровне масштабных документов стратегического планирования. В то же время как Цифровая повестка ЕАЭС, так и Основные направления ее реализации представляют собой акты общего политического характера, не обеспечивающие реального развития принципиально новых направлений интеграции в цифровой сфере.

Кроме того, согласование инициатив и одобрение проектов всеми государствами – членами ЕАЭС достаточно негативно сказывается на скорости их разработки и принятия. По этой же причине проектный подход не отличается высокой степенью вариативности: утвержденные проекты крайне сложно поддаются корректировке и изменениям, в связи с чем ошибки на этапе проработки инициатив и проектов могут привести к их полной нежизнеспособности. Здесь же можно отметить, что согласование инициатив и проектов на самом высоком политическом уровне отрицательно сказывается на связанности всех проектов между собой. Необходимость в каждом отдельном случае обсуждать и согласовывать проекты влечет за собой дробление процессов развития цифровых аспектов интеграции.

Тем не менее, несмотря на наличие отмеченных недостатков, именно такой проектный подход сегодня положен в основу цифровой трансформации ЕАЭС. Во многом выбор подобного механизма обусловлен принципом главенства суверенитета государств – членов ЕАЭС: все страны, входящие в состав ЕАЭС, в рамках заботы о национальном суверенитете оказываются вынуждены согласовывать отдельные частные инициативы в цифровой сфере.

Таким образом, документы стратегического планирования в настоящее время (помимо общих концептуальных аспектов) концентрируются на развитии практических аспектов сотрудничества государств-членов в рамках ЕАЭС. Особое внимание уделяется развитию таможенных процедур, транспортно-логистических операций, а также электронной торговли. Отдельно выделяется и сотрудничество в сфере защиты интеллектуальной собственности.

Если говорить более подробно, то в части упрощения таможенных процедур предполагается реализация целого ряда проектов, связанных с их цифровизацией.

В рамках соответствующего направления в настоящее время реализуется Проект «Экосистема цифровых транспортных коридоров ЕАЭС»[304]. Цели реализации данного проекта состоят в переходе от бумажного к электронному сопровождению транспортно-логистических операций на территории ЕАЭС. Также планируется создать сквозную интегрированную систему надзора за грузоперевозками в пространстве интеграционного объединения. Данный надзор должен осуществляться на основе анализа цифровых данных на предмет их соответствия единым стандартам транспортно-логистических сервисов. Планируется внедрение таможенного интеллектуального анализа[305]. При этом предполагается формирование системы «Единого окна» в таможенной сфере. «Единое окно» должно интегрировать в себе большинство информационных систем и ресурсов, связанных с осуществлением внешнеэкономической деятельности и таможенного контроля на таможенной территории ЕАЭС.

---

[304] Распоряжение Евразийского межправительственного совета от 31.01.2020 № 4 «О формировании экосистемы цифровых транспортных коридоров Евразийского экономического союза» // Сайт Евразийской экономической комиссии, www.eurasiancommission.org, 03.02.2020.

[305] Кузякин Ю.П., Мухин А.И. Цифровая трансформация таможенного контроля: состояние и перспективы // Юридическая наука. 2023. №8. С. 111-117.

Здесь же можно отметить проект по внедрению на уровне ЕАЭС общего цифрового технического регулирования[306]. Ключевой целью данного проекта является цифровизация процессов: формирование обязательных требований к продукции; разработка технических регламентов и перечней международных и региональных (межгосударственных) стандартов; осуществление оценки соответствия; формирование единого перечня продукции, в отношении которой устанавливаются обязательные требования в рамках ЕАЭС. При этом основным результатом реализации Проекта названо создание цифровой системы, в рамках которой всем участникам рынка будет предоставлен доступ к полной информации о проектировании, производстве и вводе продукции на рынки ЕАЭС. Кроме того, реализация Проекта также должна обеспечить сокращение затрат на процедуры проверки соответствия и на разработку технических регламентов. Иными словами, по своему содержанию формирование общего цифрового технического регулирования направлено на расширение сферы и форм обращения неперсональных данных на уровне ЕАЭС.

Впрочем, реализация соответствующих проектов идет достаточно медленно. Первоначально планировалось обеспечить формирование экосистемы цифровых транспортных коридоров в 2022 г., однако работа по соответствующему направлению ведется до сих пор. При этом отдельные инициативы в рамках соответствующего проекта находятся лишь на стадии своего концептуального оформления (например, инициативы по внедрению единой электронной международной транспортной накладной)[307]. Аналогичным образом обстоит ситуация и с внедрением цифрового

---

[306] Решение Совета Евразийской экономической комиссии от 14.07.2021 N 63 (ред. от 25.11.2022) «О реализации проекта "Цифровое техническое регулирование в рамках Евразийского экономического союза"» // Официальный сайт Евразийского экономического союза http://www.eaeunion.org/, 04.08.2021.

[307] В ЕАЭС продолжается создание экосистемы цифровых транспортных коридоров // ЕЭК: официальный сайт. 12.12.2022. [Электронный ресурс]. Режим доступа: https://eec.eaeunion.org/news/v-eaes-prodolzhaetsya-sozdanie-ekosistemy-tsifrovykh-transportnykh-koridorov/ (дата обращения: 01.02.2024).

технического регулирования. Первоначально завершение соответствующего проекта было запланировано на 2023–2024 гг., однако в текущей редакции Паспорта проекта «Цифровое техническое регулирование в рамках Евразийского экономического союза»[308] ввод наднационального компонента цифровой системы в эксплуатацию перенесен на 2025 г.

Такая же ситуация свойственна и для развития цифровых аспектов интеграции в сфере защиты интеллектуальной собственности. Несмотря на то, что необходимость охраны прав на объекты интеллектуальной собственности в сети Интернет была напрямую закреплена в Договоре о ЕАЭС, соответствующее направление интеграции до сих пор не сформировалось. В настоящее время на уровне ЕАЭС только готовится текст Соглашения о борьбе с нарушениями прав на интеллектуальную собственность в сети Интернет[309].

Тем не менее, в сфере наднационального регулирования электронной (цифровой) торговли в 2023 гг. был совершен определенный шаг вперед. 25 декабря 2023 г. был подписан Протокол о внесении изменений в Таможенный кодекс ЕАЭС[310], предусматривающий дополнение ТК ЕАЭС новыми положениями о порядке таможенного регулирования перемещения товаров электронной торговли через таможенную границу ЕАЭС. Данный протокол пока не вступил в силу и ожидает прохождения внутригосударственных процедур в государствах – членах ЕАЭС.

---

[308] Паспорт проекта «Цифровое техническое регулирование в рамках Евразийского экономического союза» (в ред. решений Совета Евразийской экономической комиссии от 17.03.2022 № 27, от 25.11.2022 № 178). [Электронный ресурс]. URL: https://www.alta.ru/tamdoc/21sr0063/ (дата обращения: 19.06.2024).

[309] Дмитрий Вольвач: страны ЕАЭС готовят соглашение по борьбе с нарушениями прав на интеллектуальную собственность в Интернете // Минэкономразвития: официальный сайт. 08.12.2023. [Электронный ресурс]. Режим доступа: https://www.economy.gov.ru/material/news/dmitriy_volvach_strany_eaes_gotovyat_soglashenie_po_borbe_s_narusheniyami_prav_na_intellektualnuyu_sobstvennost_v_internete.html (дата обращения: 01.02.2024).

[310] Протокол о внесении изменений в Договор о Таможенном кодексе Евразийского экономического союза от 11 апреля 2017 г. (Санкт-Петербург, 25 декабря 2023 г.) (не вступил в силу) // Официальный сайт Евразийского экономического союза http://www.eaeunion.org/, 28.12.2023.

В соответствии с изменениями, вносимыми Протоколом, предполагается закрепление в ТК ЕАЭС:

- новой категории товаров – товаров электронной торговли;

- нового субъекта электронной торговли – оператора электронной площадки;

- особого режима таможенного декларировании на основе подачи декларации на товары электронной торговли;

- новой формы таможенного хранения товаров в виде таможенных («бондовых») складов.

Так, в частности, товары электронной торговли разделены на две категории: 1) товары электронной торговли, предназначенные для реализации физическим лицам (пп. 47.2 ч. 1 ст. 2 будущей редакции ТК ЕАЭС) и 2) товары электронной торговли, приобретенные физическими лицами (пп. 47.3 ч. 1 ст. 2 будущей редакции ТК ЕАЭС).

Обе категории товаров связаны с осуществлением онлайн-торговли посредством различных интернет-площадок (т.н. маркетплейсов). Товары электронной торговли, предназначенные для реализации физическим лицам, должны быть предназначены для реализации с использованием электронных торговых площадок. В свою очередь, товары электронной торговли, приобретаемые физическими лицами, должны приобретаться с использованием электронных торговых площадок.

При этом обязательным критерием для отнесения товаров к любой из данных категорий является участие физических лиц в сделках по их реализации или приобретению:

- потенциальное, когда товары ввозятся на таможенную территорию ЕАЭС для последующей продажи физическим лицам на интернет-площадках;

- реальное, когда товары были заказаны самими физическими лицами-резидентами ЕАЭС на зарубежных интернет-площадках или иностранными

физическими лицами у резидентов ЕАЭС на евразийских интернет-площадках[311].

В то же время сделки купли-продажи товаров электронной торговли не могут заключаться между физическими лицами. Если обе стороны сделки являются физическими лицами, несмотря на использование маркетплейса (электронной торговой площадки) в качестве информационного посредника, приобретенные товары не будут квалифицироваться в качестве товаров электронной торговли[312].

Таким образом, одна сторона сделок купли-продажи (в рамках реализации товаров или в рамках их приобретения) товаров электронной торговли всегда должна быть физическим лицом (потребителем), а другая сторона никогда не может быть физическим лицом[313].

Целесообразность введения данного ограничения вызывает достаточно серьезные сомнения, поскольку участниками электронной торговли на маркетплейсах достаточно часто являются физические лица. Возможности маркетплейсов по распространению товаров и продвижению их среди большого круга лиц создают выгодные возможности, прежде всего, именно для субъектов малого и среднего бизнеса. При этом в качестве соответствующих субъектов могут выступать индивидуальные предприниматели и самозанятые (физические лица)[314].

Представляется, что на уровне правоприменительной практики ИП все же не будут квалифицироваться как физические лица. Скорее всего, они будут отнесены к профессиональным участникам гражданского оборота, что позволит им импортировать на таможенную территорию ЕАЭС товары электронной торговли для последующей реализации физическим лицам посредством маркетплейсов. В то же время на уровне текста

---

311 Лю К.А. Новый порядок регулирования внешней электронной торговли в ЕАЭС: новеллы таможенного законодательства // Инновации и инвестиции. 2024. № 2. С. 69–74.
312 Там же. С. 71.
313 Там же.
314 Лю К.А. Указ. соч. С. 72.

законодательных новелл ТК ЕАЭС соответствующая возможность не закреплена.

Что же касается самозанятых, то в силу своего правового статуса они однозначно относятся к физическим лицам, занимающимся профессиональной деятельностью, приносящей доход. Как следствие, самозанятые точно не смогу воспользоваться особым правовым режимом при импорте товаров электронной торговли на таможенную территорию ЕАЭС в целях их последующей реализации физическим лицам.

Впрочем, на этом проблемы вносимых в ТК ЕАЭС изменений не заканчиваются.

В соответствии с ч. 2 ст. 309.1 будущей редакции ТК ЕАЭС, планируется закрепить запрет на использование товаров электронной торговли в коммерческой деятельности после их реализации физическим лицам под угрозой привлечения к юридической ответственности в соответствии с национальным законодательством государства – члена ЕАЭС (на территории которого осуществлялась соответствующая коммерческая деятельность). Соответствующий запрет начинает действовать после выпуска товаров на таможенную территорию ЕАЭС и фактически распространяется на физических лиц, которые приобрели товары электронной торговли[315].

С одной стороны, установление подобного запрета направлено на предотвращение потенциальных злоупотреблений новым таможенным режимом товаров электронной торговли. Предполагается, что недобросовестные импортеры (или экспортеры) не смогут дробить собственные сделки поставки товаров между фиктивными физическими лицами – получателями товаров, чтобы снизить таможенную нагрузку[316].

Однако соответствующие действия недобросовестных импортеров (экспортеров) не требуют установления дополнительных запретов и ограничений. И в отсутствие запрета на использование товаров электронной

[315] Там же.
[316] Лю К.А. Указ. соч. С. 72.

торговли в коммерческой деятельности соответствующие лица находились бы под угрозой привлечения к уголовной или административной ответственности за уклонение от уплаты таможенных платежей и нарушение таможенного законодательства[317].

С другой стороны, в рамках запрета использовать полученные товары электронной торговли в коммерческой деятельности можно заметить некритичное восприятие положений законодательства о правах потребителей. Представляется, что в ч. 2 ст. 309.1 будущей редакции ТК ЕАЭС авторы изменений несколько некорректно воспроизвели норму о приобретении товаров для личного использования[318].

Однако сфера электронной торговли посредством маркетплейсов не может быть в полной мере урегулирована нормами законодательства о защите прав потребителей. Электронная торговля с использованием цифровых торговых площадок представляет собой разноаспектную сферу общественной жизни, в рамках которой товары могут приобретаться не только для личного использования[319].

Более того, формально-юридически текст изменений ТК ЕАЭС предусматривает возможность приобретения товаров электронной торговли такими физическими лицами, как индивидуальные предприниматели и самозанятые. В то же время использовать соответствующие товары в рамках коммерческой деятельности такие субъекты не смогут в силу прямого запрета ч. 2 ст. 309.1 будущей редакции ТК ЕАЭС.

Получается, что ИП или самозанятый при заказе товаров онлайн на зарубежных маркетплейсах должны особым образом уведомить продавца и оператора электронной торговой площадки о том, что приобретаемые товары будут использоваться в коммерческой деятельности и в отношении них не подлежит применению особая таможенная процедура, установленная для

---

[317] Там же.
[318] Там же.
[319] Там же.

товаров электронной торговли. В свою очередь, при заказе товаров на отечественных маркетплейсах ИП или самозанятый вообще не могут приобрести для коммерческой деятельности товары, ввезенные в соответствии с особой таможенной процедурой товаров электронной торговли (в силу прямого запрета на использование товаров электронной торговли в коммерческой деятельности. закрепленного в ч. 2 ст. 309.1 будущей редакции ТК ЕАЭС)[320].

При этом стоит учитывать, что товары электронной торговли, предназначенные для реализации физическим лицам, могут квалифицироваться в качестве таковых только в тех случаях, когда собственником данных товаров является иностранное лицо. Товары электронной торговли, которые при ввозе на таможенную территорию находятся в собственности резидентов ЕАЭС, не подпадают под правовой режим товаров электронной торговли (ч. 4 ст. 309.1 будущей редакции ТК ЕАЭС). Они импортируются и впоследствии реализуются на таможенной территории ЕАЭС в соответствии с общей таможенной процедурой.

Иностранное лицо, собственник товаров электронной торговли, не несет никакой ответственности за реализацию товаров физическим лицам, которые впоследствии будут использовать их в коммерческой деятельности. Не установлена ответственность и для оператора электронной торговли. Оператор лишь собирает всю информацию, необходимую для прохождения специальной таможенной процедуры, устанавливаемой в отношении товаров электронной торговли. При этом оператор может изменять или дополнять соответствующую информацию (ст. 429.4 будущей редакции ТК ЕАЭС). Зона ответственности оператора электронной торговли строго ограничена совершением таможенных процедур. Использование товаров электронной торговли в коммерческой деятельности после их выпуска на таможенную территорию ЕАЭС оператора не касается.

---

[320] Лю К.А. Указ. соч. С. 72.

Как следствие, именно ИП или самозанятый при приобретении товаров на отечественных маркетплейсах будет обязан проверять, по итогам какой именно таможенной процедуры они реализуются на маркетплейсах. В условиях отсутствия публично достоверной информации обо всех таможенных операциях вероятность успешного завершения подобной проверки достаточно низка. Соответственно, подавляющее большинство товаров на отечественных маркетплейсах, реализуемых иностранными резидентами, окажутся официально недоступны для ИП и самозанятых[321].

Подобный социально-экономический эффект нового наднационального регулирования нельзя назвать положительным.

Отмеченные выше недостатки, скорее всего, будут компенсироваться необязательностью исполнения требований новой редакции ТК ЕАЭС о запрете на осуществление коммерческой деятельности, ввиду отсутствия эффективных средств контроля со стороны органов государственной власти.

Потенциально соответствующий контроль может осуществляться ФНС России в рамках проведения налоговых проверок профессиональных участников предпринимательской деятельности, а также самозанятых. В случае выявления фактов использования товаров электронной торговли в коммерческой деятельности ФНС России могла бы передавать соответствующую информацию ФТС России для доначисления таможенных платежей и привлечения виновных лиц к ответственности за уклонение от уплаты таможенных платежей.

Однако администрирование соответствующей контрольно-надзорной деятельности неизбежно потребует чрезмерных затрат, несоизмеримых с потенциальной выгодой для бюджета. Как следствие, видится маловероятным, что соблюдение запрета на использование товаров электронной торговли в коммерческой деятельности будет строго контролироваться. Представляется, что привлечение к ответственности за

[321] Лю К.А. Указ. соч. С. 72.

нарушение данного запрета будет осуществляться выборочно в отношении лиц, закупающих товары электронной торговли для осуществления коммерческой деятельности в особо крупных объемах, и в отношении лиц, деятельность которых стала предметом налоговой проверки по иным основаниям.

Также весьма вероятно, что правоприменительная практика скорректирует и положения о запрете на заключение сделок с товарами электронной торговли между физическими лицами (вполне возможным видится разрешение совершения подобных сделок с участием индивидуальных предпринимателей или иных иностранных субъектов индивидуального предпринимательства).

Некоторым плюсом вносимых в ТК ЕАЭС изменений является признание особого правового статуса за операторами электронных торговых площадок[322]. Его конкретизацию предполагается осуществить в Главе 60.1 будущей редакции ТК ЕАЭС.

Оператор электронной торговли осуществляет таможенные операции в отношении товаров электронной торговли: в отношении товаров, приобретенных физическими лицами — от их имени; а в отношении товаров, ввозимых в целях реализации физическим лицам — от своего имени (ч. 1 ст. 429.1 будущей редакции ТК ЕАЭС). Также в случаях, когда по истечении срока временного хранения товары, приобретенные физическими лицами, не были задекларированы, оператор электронной торговли является декларантом по таможенным процедурам отказа в пользу государства или уничтожения (абз. 2 ч. 1 ст. 309.4 будущей редакции ТК ЕАЭС)

Товары электронной торговли, ввозимые в целях реализации физическим лицам на маркетплейсах, подпадают под процедуру таможенного склада. Товары, приобретенные физическими лицами, при

[322] Лю К.А. Указ. соч. С. 73.

прохождении таможенной границы могут помещаться под процедуру таможенного склада или помещаться на временное хранение.

Оператор ведет раздельный учет 1) предназначенных для реализации товаров, находящихся под процедурой таможенного склада; 2) приобретенных физическими лицами товаров, находящихся под процедурой таможенного склада; 3) приобретенных физическими лицами товаров, находящихся на временном хранении (п.п. 7-8 ч. 1 ст. 429.5 будущей редакции ТК ЕАЭС). При этом оператор электронной торговли может добровольно ограничить сферу своей деятельности только одной категорией товаров электронной торговли (товарами, реализуемыми физическим лицам, или товарами, приобретаемыми физическими лицами).

В целом правовой статус оператора электронной торговли действительно соответствует общим особенностям осуществления трансграничной торговли с использованием маркетплейсов. Действительно, товары, реализуемые на подобных интернет-площадках, хранятся на складах их операторов. Перевозка товаров также осуществляется операторами электронной торговли. Ни покупатель, ни продавец в рамках подобного формата электронной торговли не занимаются перевозкой товаров, в связи с чем ответственность за совершение таможенных процедур здесь вполне логично возложена на оператора электронной торговли[323].

В подобных условиях создание особого режима таможенного склада для товаров электронной торговли видится достаточно эффективным и актуальным решением. Учитывая стремление маркетплейсов к укрупнению и постоянному масштабированию, создание подобных буферных таможенных зон может позволить оптимизировать трансграничную (внешнюю) электронную торговлю. Действующие крупные операторы будут официально

[323] Лю К.А. Указ. соч. С. 73.

создавать таможенные склады и на легальной основе выстраивать постоянное взаимодействие с таможенными органами[324].

Также стоит отметить, что оператор электронной торговли обязан не разглашать персональные данные («конфиденциальную информацию») получателей товаров, а также иные сведения о них, составляющие охраняемую законом тайну (п. 2 ч. 1 ст. 429.5 будущей редакции ТК ЕАЭС). Данную обязанность можно рассматривать как одно из первых проявлений защиты персональных данных в сети Интернет на наднациональном уровне ЕАЭС. Впрочем, для формирования полноценной системы защиты персональных данных в соответствующей сфере требуется установление специальных правил сбора, хранения, оборота и уничтожения персональных данных, а также ответственности операторов за их разглашение[325].

Все вышеизложенное позволяет рассматривать изменения, вносимые в Таможенный кодекс ЕАЭС в качестве первого существенного шага на пути формирования принципиально нового направления наднационального регулирования цифрового пространства, хотя в соответствующей сфере требуется проведение большого количества работы.

Общеправовая база соответствующих изменений проработана крайне слабо, в отдельных частях противоречит реалиям общественных отношений в цифровой среде и создает риски привлечения к ответственности добросовестных участников оборота.

Представляется, что использование видоизмененных конструкций законодательства о защите прав потребителей не отвечает фактическому содержанию всех правоотношений, возникающих в рамках электронной торговли с использованием маркетплейсов. Более корректным здесь видится формирование нового специального правового режима трансграничной электронной торговли, который бы учитывал специфику всех торговых операций, совершаемых на соответствующих платформах.

---

[324] Лю К.А. Указ. соч. С. 73.
[325] Там же.

В целом именно на это ориентирован и правовой режим оператора электронной торговли, который учитывает разные аспекты совершаемых в рамках такой торговли операций и предусматривает определенную дифференциацию правовых средств и таможенных процедур в зависимости от реального содержания правоотношений между продавцом и покупателем.

Если же оставаться в рамках существующей логики изменений ТК ЕАЭС, то необходимо доработать категориальный аппарат и юридическую технику новых норм[326]:

- категория «физическое лицо» должна быть исключена из норм об электронной торговле с использованием электронных торговых площадок;

- категория «лицо», которой обозначается продавец/поставщик по сделкам с товарами электронной торговли, должна быть заменена на категорию «резидент ЕАЭС» и категорию «резидент третьей страны» соответственно контексту использования в нормах ТК ЕАЭС;

- должен быть снят запрет на совершение сделок купли-продажи/поставки между физическими лицами;

- должен быть снят запрет на использование товаров электронной торговли в коммерческой деятельности после их выпуска на таможенную территорию ЕАЭС.

Таким образом, товарами электронной торговли должны признаваться[327]:

1) товары, приобретаемые резидентами ЕАЭС у иностранных продавцов/поставщиков на электронных торговых площадках с использованием сети Интернет;

2) товары, приобретаемые резидентами третьих стран у продавцов/поставщиков из государств – членов ЕАЭС на электронных торговых площадках с использованием сети Интернет;

---

[326] Лю К.А. Новый порядок регулирования внешней электронной торговли в ЕАЭС: новеллы таможенного законодательства // Инновации и инвестиции. 2024. № 2. С. 69-74.
[327] Лю К.А. Указ. соч. С. 73.

3) товары, предназначенные для реализации на таможенной территории ЕАЭС на электронных торговых площадках с использованием сети Интернет.

Кроме того, необходимо конкретизировать правовой статус операторов электронной торговли. Несмотря на то, что соответствующим аспектам предполагается посвятить отдельную Главу 60.1 ТК ЕАЭС, в тексте изменений отсутствует определение оператора электронной торговли.

Представляется, что с учетом масштабов деятельности и значимости полного раскрытия информации о своей деятельности оператор электронной торговли может пониматься как публичное акционерное общество (или иностранное юридическое лицо иной организационно-правовой формы, предполагающей публичное раскрытие информации об осуществляемой деятельности), включенное в реестр операторов электронной торговли в соответствии с Таможенным кодексом ЕАЭС, которое владеет и управляет электронной торговой площадкой, посредством которой обеспечивается дистанционное заключение договоров купли-продажи или поставки товаров электронной торговли (в том числе с участием потребителей)[328].

При этом под электронной торговой площадкой следует понимать совокупность информационно-коммуникационных технологий, сервисов, а также обеспечивающих программно-аппаратных средств, посредством которых обеспечивается функционирование цифровых онлайн-ресурсов (сайтов в сети Интернет, мобильных приложений и иных), предназначенных для осуществления дистанционного заключения договора купли-продажи или поставки товаров.

Кроме того, в настоящее время не определен ряд важных обязанностей и сфер ответственности операторов электронной торговли. Подобный подход обусловлен, прежде всего, внесением изменений именно в Таможенный кодекс, который естественным образом концентрируется именно на особенностях осуществления таможенных операций и на порядке

[328] Там же.

прохождения таможенных процедур. Тем не менее введение в правовое поле ЕАЭС принципиально новой категории «оператор электронной торговли» неизбежно требует ее конкретизации. Правовой режим оператора электронной торговли в настоящий момент связывается именно с перемещением товаров через таможенную границу, поэтому его уточнение можно осуществить и в рамках ТК ЕАЭС[329].

Так, в частности, предлагается дополнить обязанности оператора электронной торговли (ст. 429.5 будущей редакции ТК ЕАЭС) следующими основными пунктами[330]:

- оператор электронной торговли осуществляет сбор и размещение на своем сайте все необходимой информации о продавцах/поставщиках товаров электронной торговли, сведения о прохождении процедур сертификации и стандартизации ЕАЭС;

- оператор электронной торговли размещает сведения о типе и виде таможенных процедур, по которым товары электронной торговли подлежат выпуску на таможенной территории ЕАЭС (соответствующая информация должна аккумулироваться в рамках публично достоверных реестров ИИС ЕАЭС);

- в случае выявления товаров электронной торговли, реализация которой не соответствует законодательству ЕАЭС или государств – членов ЕАЭС, оператор электронной торговли обязан уведомить о выявленных нарушениях покупателей данных товаров, а также таможенные органы, уполномоченные органы ЕАЭС и уполномоченные органы государств – членов ЕАЭС, на территории которых были реализованы соответствующие товары (по информации, имеющейся у оператора электронной торговли); реализация товаров, не соответствующих законодательству ЕАЭС, должна быть приостановлена.

---

[329] Лю К.А. Указ. соч. С. 73.
[330] Там же.

В целом предлагаемый подход с некоторой дополнительной корректировкой положений об операторах электронной торговли позволит более полно урегулировать общественные отношения, возникающие в рамках трансграничной торговли с использованием электронных торговых площадок[331].

При этом важно подчеркнуть, что сам факт дополнения ТК ЕАЭС новыми положениями, непосредственно связанными с цифровой сферой, свидетельствует о верном направлении развития наднационального правового регулирования. Несмотря на то, что соответствующие нормы затрагивают лишь часть общественных отношений, связанных с торговлей товарами на интернет-площадках, они все же обозначают новый вектор расширения цифровых аспектов интеграции в рамках ЕАЭС.

Учитывая сложный процесс согласования конкретных планов действий по развитию цифровых аспектов интеграции (не в рамках общих политических заявлений или отдельных узких проектов), можно сделать вывод, что именно дальнейшее совершенствование наднационального регулирования таможенных процедур в отношении товаров электронной торговли сегодня является наиболее перспективным направлением расширения цифровых компетенций ЕАЭС.

Впрочем, как можно заметить, соответствующее направление развития охватывает лишь весьма ограниченную сферу насущных вопросов в сфере наднационального регулирования цифрового пространства. При этом, если суммировать проведенный анализ наднационального регулирования цифрового пространства в ЕАЭС, можно сделать следующий *вывод*: в настоящее время цифровое пространство на уровне ЕАЭС регулируется достаточно фрагментарно. Набор институтов и механизмов соответствующего регулирования не в полной мере соответствует технологическим вызовам современной цифровой эпохи. При этом

[331] Лю К.А. Указ. соч. С. 74.

формирование новых аспектов цифровой интеграции ЕАЭС идет медленно (что во многом обусловлено действием принципа главенства суверенитета государств – членов ЕАЭС).

В полной мере на уровне ЕАЭС реализовано лишь одно направление – цифровой оборот статистической государственной информации и иных неперсональных данных в сферах, связанных с общими рынками ЕАЭС, общей таможенной территорией ЕАЭС, свободой передвижения рабочей силы и промышленной координацией. Работа по данному направлению идет достаточно активно. Формируется «трансграничное пространство доверия», непосредственной формой которого выступает Интегрированная информационная система ЕАЭС. При этом приоритет получают проекты, связанные с цифровизацией таможни, таможенного регулирования, транзита товаров по территории ЕАЭС и с управлением транспортно-логистическими операциями.

В общем виде на уровне ЕАЭС регулируются цифровые аспекты осуществления государственных закупок, связанные с проведением закупок на электронных площадках и с размещением всей информации о закупках в сети Интернет (наибольшая гармонизация по данному направлению достигнута в части использования единой электронной цифровой подписи поставщиков). В то же время на наднациональном уровне устанавливаются лишь общие концептуальные аспекты электронных закупок. Приоритет отдается национальному законодательству и политической воле государств-членов.

Аналогичным образом лишь в рамках общих правил и принципов защиты конкуренции действует антимонопольное регулирование на цифровых рынках и рынках цифровых услуг. Здесь наднациональное законодательство не устанавливает специальных требований или ограничений, подлежащих применению именно в цифровой сфере. Более того, положения XVIII Договора о ЕАЭС всю полноту регулирования в сфере

конкурентной политики предоставляют государствам - членам ЕАЭС, ограничивая интеграционный уровень только общей координацией и согласованием национальных политик.

Крайне фрагментарно на уровне ЕАЭС регулируются вопросы, связанные с защитой интеллектуальной собственности в цифровом пространстве. Специального регулирования соответствующих общественных отношений в сети Интернет на уровне ЕАЭС в настоящее время не сформировано. Защита интеллектуальной собственности в цифровом пространстве обеспечивается при помощи традиционных правовых средств. Напрямую с цифровой сферой связаны лишь положения наднационального законодательства о защите прав на программы для ЭВМ и на топологии интегральных микросхем. В настоящее время на уровне ЕАЭС только готовится текст Соглашения о борьбе с нарушениями прав на интеллектуальную собственность в сети Интернет.

Обеспечение стабильного функционирования и безопасности цифровой инфраструктуры заявлено как одно из основных направлений реализации Цифровой повестки ЕАЭС на период до 2025 г. Однако непосредственных шагов по реализации данного направления сделано не было. Сфера цифровой безопасности слишком чувствительна для государств – членов ЕАЭС, в связи с чем они не спешат согласовывать свои усилия на наднациональном уровне (что вполне укладывается в логику принципа господства суверенитета государств-членов). Косвенно обеспечению безопасности цифровой инфраструктуры способствует завершение формирования общего рынка электроэнергии ЕАЭС, однако по своему содержанию и целям соответствующий общий рынок достаточно слабо связан непосредственно с цифровыми технологиями.

Цифровизация экономики, рынков товаров, работ, услуг и капиталов также представляет собой одной из основных направлений реализации Цифровой повестки ЕАЭС. Однако работа по соответствующему

направлению ведется точечно, в рамках отдельных проектов. Так, помимо цифровизации транзита в настоящее время реализуются проекты «Работа без границ» и «Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий». В целом прогресс по данному направлению может быть оценен как незначительный.

Впрочем, в конце 2023 г. на наднациональном уровне были согласованы существенные дополнения таможенного законодательства ЕАЭС в части наднационального регулирования внешней (с участием резидентов третьих стран) электронной торговли. Так, после прохождения национальных процедур, необходимых для вступления в силу предлагаемых изменений, Таможенный кодекс ЕАЭС будет дополнен целым блоком норм, посвященных правовому режиму товаров электронной торговли. Кроме того, будет создан особый правовой режим для операторов электронной торговли, а также будет расширен правовой режим таможенного склада.

Новые статьи ТК ЕАЭС в части обязанностей оператора электронной торговли предполагают также внедрение первой наднациональной нормы об охране персональных данных. Так, планируется установить обязанность операторов электронной торговли не разглашать персональные данные покупателей и иные сведения, составляющие охраняемую законом тайну. С точки зрения содержания, данную норму сложно назвать прогрессивной, однако с точки зрения наличия на уровне ЕАЭС норм о персональных данных, она представляет собой важный шаг вперед.

Что же касается наднационального регулирования цифровых рынков и цифровых услуг, а равно искусственного интеллекта и криптоактивов, то соответствующие направления в настоящее время = практически никак не представлены на уровне ЕАЭС. Упоминание об отдельных инициативах в соответствующих отраслях можно встретить лишь на уровне общих политических документов, заявлений и публикаций.

Заключение

Завершая настоящее исследование, исходя из цели и задач, обозначенных во введении, представляется возможным сформулировать следующие основные выводы об особенностях наднационального регулирования цифрового пространства в ЕС и в ЕАЭС на современном этапе.

Формирование наднационального регулирования цифрового пространства в ЕС осуществлялось в рамках трех последовательных этапов:

1. этап зарождения регулирования цифрового пространства (2010–2014 гг.). На данном этапе основное внимание было сосредоточено на формировании гармонизированной системы публичных закупок в электронной форме, а также на совершенствовании общеевропейской системы защиты интеллектуальной собственности и авторских прав в сети Интернет (при этом здесь были использованы достаточно нестандартные механизмы мягкого рыночного влияния на участников цифровых рынков за счет принятия ими на себя добровольных обязательств перед правообладателями при посредничестве Еврокомиссии). Тем не менее, несмотря на предпринятые шаги, наднациональное регулирование цифрового пространства все еще носило крайне фрагментарный характер и не затрагивало большого количества сфер цифровой общественной жизни, имеющих принципиальное значение для развития европейской интеграции (в частности, речь здесь идет об отсутствии наднационального регулирования цифровых рынков и цифровых услуг, обращения цифровых данных, кибербезопасности и т.д.);

2. этап фрагментарного регулирования цифрового пространства (2015–2019 гг.). В рамках данного этапа развития наднационального правового регулирования цифрового пространства в ЕС было обеспечено существенное расширение сфер соответствующего регулирования по сравнению с предыдущим этапом. Так, в частности, в период с 2014 г. по 2019 г. были

обеспечены разработка и принятие актов ЕС в сфере защиты и обращения персональных и неперсональных данных, а также в сфере кибербезопасности. При этом принятые в рамках соответствующего этапа Общий регламент по защите данных 2016 г., Регламент в сфере обращения неперсональных данных на территории ЕС 2018 г., Директива по безопасности сетей и информационных систем 2016 г., Регламент о кибербезопасности 2019 г. стали ключевыми актами в соответствующих сферах, сформировав наиболее принципиальные черты правового режима защиты и обращения данных в сети Интернет, а также обеспечив внедрение современного общеевропейского подхода к обеспечению кибербезопасности;

3. этап всеобъемлющего регулирования цифрового пространства (2020 г. – н.в.). Данный этап развития наднационального регулирования цифрового пространства в ЕС характеризуется переходом к формированию принципиально новых масштабных направлений интеграции в цифровой сфере. К подобным направлениям, в частности, относятся создание правовой базы для функционирования единого рынка цифровых услуг ЕС, а также для единообразного применения технологий искусственного интеллекта в государствах – членах ЕС и для единообразного регулирования рынка криптоактивов.

Кроме того, на современном этапе свое углубление и расширение получили и традиционные направления наднационального регулирования цифрового пространства в ЕС в таких сферах, как защита интеллектуальной собственности в сети Интернет, обеспечение кибербезопасности, защита и оборот неперсональных данных, обеспечение стабильности и безопасности цифровой (а именно облачной) инфраструктуры, гармонизация правил осуществления публичных закупок в электронной форме и закупок цифровых товаров и услуг.

При этом развитие наднационального регулирования цифрового пространства в ЕС осуществляется по трем основным направлениям: 1) цифровая среда; 2) цифровая инфраструктура; 3) цифровой рынок.

В рамках первого направления в настоящее время предполагается разработка и внедрение новых стандартов кибербезопасности и обращения с персональными данными на уровне ЕС. При этом данные стандарты должны будут распространяться как на внутренних (резидентов ЕС), так и на внешних участников цифрового рынка. Общей нормативной основой для внедрения новых стандартов кибербезопасности должно стать внесение изменений в Директиву о безопасности сетей и информационных систем 2016 г. В части защиты персональных данных в цифровой среде сегодня ведется работа по созданию и принятию стандартов и инструкций в сфере усиленной защиты персональных данных в наиболее чувствительных сферах общественной жизни (финансовом секторе, здравоохранении и др.), а к 2030 г. планируется полностью модернизировать систему защиты персональных данных таким образом, чтобы она обеспечивала высокий уровень защиты данных и конфиденциальности вне зависимости от конкретных обстоятельств хранения и обработки таких данных.

Второе направление представлено преимущественно положениями Европейской стратегии данных 2020 г., устанавливающей необходимость разработки и принятия наднациональных правил создания и функционирования облачной инфраструктуры, которые бы обеспечили создание конкурентных условий сбора, анализа, обработки и обмена неперсональными данными для резидентов ЕС. При этом в основу такого регулирования положен принцип открытого доступа к государственным и наднациональным данным в отдельных стратегических секторах (в частности, в сфере транспорта и здравоохранения). Кроме того, в сферу правового регулирования цифровой инфраструктуры были инкорпорированы требования обеспечения нулевого уровня выбросов парниковых газов и

энергоэффективности посредством возложения на Еврокомиссию обязанности разработать новые расширенные индексы цифровой экономики и общества (DESI).

В рамках реализации третьего направления в 2022 г. на уровне ЕС был создан единый рынок цифровых услуг, а также были сформированы единые требования о конкурентных и справедливых рынках в цифровом секторе. Данный шаг ознаменовал собой значительное расширение правового регулирования соответствующих рынков на уровне ЕС, которое до 2022 г. осуществлялось в соответствии с национальными законодательствами государств-членов.

При этом в рамках ключевых для этой сферы Регламента о едином рынке цифровых услуг и Регламента о конкурентных и справедливых рынках в цифровом секторе были сформированы современные эффективные правила, обеспечивающие 1) защиту авторских прав и интеллектуальной собственности в цифровой среде с учетом актуальных вызовов цифровой эпохи; 2) адекватное цифровой сфере антимонопольное регулирование, учитывающее, в том числе, современные вызовы для цифрового суверенитета ЕС и ведения IT-деятельности субъектами малого и среднего предпринимательства в ЕС; 3) свободное движение цифровых услуг на едином рынке ЕС (включая посреднические услуги по передаче, хранению, распределению или размещению информации в сети Интернет).

Также в 2023 г. был принят Регламент о рынках криптоактивов, призванный обеспечить всеобъемлющее правовое регулирование криптоактивов (с учетом как их внутренней дифференциации, так и их внешнего отграничения от традиционных финансовых инструментов).

В дополнение к отмеченным регламентам сегодня на уровне ЕС проходит процедура принятия Регламента об искусственном интеллекте. В соответствии с данным регламентом планируется внедрить на уровне ЕС

коммунитарные требования к созданию, реализации и пользованию системами ИИ.

Что касается ЕАЭС, то в настоящее время цифровое пространство на уровне ЕАЭС регулируется достаточно фрагментарно. Набор институтов и механизмов соответствующего регулирования не в полной мере соответствует технологическим вызовам современной цифровой эпохи. При этом формирование новых аспектов цифровой интеграции ЕАЭС идет медленно (что во многом обусловлено действием принципа главенства суверенитета государств – членов ЕАЭС).

В полной мере на уровне ЕАЭС реализовано лишь одно направление — цифровой оборот статистической государственной информации и иных неперсональных данных в сферах, связанных с общими рынками ЕАЭС, общей таможенной территорией ЕАЭС, свободой передвижения рабочей силы и промышленной координацией. Работа по данному направлению идет достаточно активно. Формируется «трансграничное пространство доверия», непосредственной формой которого выступает Интегрированная информационная система ЕАЭС. При этом приоритет получают проекты, связанные с цифровизацией таможни, таможенного регулирования, транзита товаров по территории ЕАЭС и с управлением транспортно-логистическими операциями.

В общем виде на уровне ЕАЭС регулируются цифровые аспекты осуществления государственных закупок, связанные с проведением закупок на электронных площадках и с размещением всей информации о закупках в сети Интернет (наибольшая гармонизация по данному направлению достигнута в части использования единой электронной цифровой подписи поставщиков). В то же время на наднациональном уровне устанавливаются лишь общие концептуальные аспекты электронных закупок. Приоритет отдается национальному законодательству и политической воле государств-членов.

Аналогичным образом лишь в рамках общих правил и принципов защиты конкуренции действует антимонопольное регулирование на цифровых рынках и рынках цифровых услуг. Здесь наднациональное законодательство не устанавливает специальных требований или ограничений, подлежащих применению именно в цифровой сфере. Более того, положения XVIII Договора о ЕАЭС всю полноту регулирования в сфере конкурентной политики предоставляют государствам – членам ЕАЭС, ограничивая интеграционный уровень только общей координацией и согласованием национальных политик.

Крайне фрагментарно на уровне ЕАЭС регулируются вопросы, связанные с защитой интеллектуальной собственности в цифровом пространстве. Специального регулирования соответствующих общественных отношений в сети Интернет на уровне ЕАЭС в настоящее время не сформировано. Защита интеллектуальной собственности в цифровом пространстве обеспечивается при помощи традиционных правовых средств. Напрямую с цифровой сферой связаны лишь положения наднационального законодательства о защите прав на программы для ЭВМ и на топологии интегральных микросхем. В настоящее время на уровне ЕАЭС только готовится текст Соглашения о борьбе с нарушениями прав на интеллектуальную собственность в сети Интернет.

Обеспечение стабильного функционирования и безопасности цифровой инфраструктуры заявлено как одно из основных направлений реализации Цифровой повестки ЕАЭС на период до 2025 г. Однако непосредственных шагов по реализации данного направления сделано не было. Сфера цифровой безопасности слишком чувствительна для государств – членов ЕАЭС, в связи с чем они не спешат согласовывать свои усилия на наднациональном уровне (что вполне укладывается в логику принципа господства суверенитета государств-членов). Косвенно обеспечению безопасности цифровой инфраструктуры способствует завершение формирования общего рынка

электроэнергии ЕАЭС, однако по своему содержанию и целям соответствующий общий рынок достаточно слабо связан непосредственно с цифровыми технологиями.

Цифровизация экономики, рынков товаров, работ, услуг и капиталов также представляет собой одно из основных направлений реализации Цифровой повестки ЕАЭС. Однако работа по соответствующему направлению ведется точечно, в рамках реализации отдельных проектов. Так, помимо цифровизации транзита в настоящее время реализуются проекты «Работа без границ» и «Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий». В целом прогресс по данному направлению может быть оценен как незначительный.

Впрочем, в конце 2023 г. на наднациональном уровне были согласованы существенные дополнения таможенного законодательства ЕАЭС в части наднационального регулирования внешней (с участием резидентов третьих стран) электронной торговли. После прохождения национальных процедур, необходимых для вступления в силу предлагаемых изменений, Таможенный кодекс ЕАЭС будет дополнен целым блоком норм, посвященных правовому режиму товаров электронной торговли. Кроме того, будет создан особый правовой режим для операторов электронной торговли, а также будет расширен правовой режим таможенного склада.

Кроме того, новые статьи ТК ЕАЭС в части обязанностей оператора электронной торговли предполагают внедрение первой наднациональной нормы об охране персональных данных. Так, предполагается установить обязанность операторов электронной торговли не разглашать персональные данные покупателей, а также иные сведения, составляющие охраняемую законом тайну. С точки зрения содержания, данную норму сложно назвать прогрессивной, однако, с точки зрения наличия на уровне ЕАЭС норм о персональных данных, она представляет собой важный шаг вперед.

Что же касается наднационального регулирования цифровых рынков и цифровых услуг, а равно искусственного интеллекта и криптоактивов, то соответствующие направления в настоящее время практически никак не представлены на уровне ЕАЭС. Упоминание об отдельных инициативах в соответствующих отраслях можно встретить лишь на уровне общих политических документов, заявлений и публикаций.

Список использованных источников и литературы

Акты ЕС и ЕАЭС

1. Договор о Евразийском экономическом союзе (Подписан в г. Астане 29.05.2014) // Официальный сайт Евразийской экономической комиссии. [Электронный ресурс]. URL: http://www.eurasiancommission.org/. – 05.06.2014.
2. Решение Высшего Евразийского экономического совета от 11.10.2017 N 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» // Официальный сайт Евразийского экономического союза [Электронный ресурс]. URL: http://www.eaeunion.org/. – 10.11.2017.
3. Решение Евразийского межправительственного совета от 01.02.2019 N 1 «О механизмах реализации проектов в рамках цифровой повестки Евразийского экономического союза» // Официальный сайт Евразийского экономического союза [Электронный ресурс]. URL: http://www.eaeunion.org/. – 18.02.2019.
4. Решение Евразийского межправительственного совета от 30 апреля 2019 года № 2 «О реализации проекта "Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий"» // Официальный сайт Евразийского экономического союза [Электронный ресурс]. URL: www.eaeunion.org. – 06.05.2019.
5. Распоряжение Евразийского межправительственного совета от 31.01.2020 № 4 «О формировании экосистемы цифровых транспортных коридоров Евразийского экономического союза» // Сайт Евразийской экономической комиссии [Электронный ресурс]. URL: www.eurasiancommission.org. – 03.02.2020.
6. Решение Коллегии Евразийской экономической комиссии от 06.09.2022 № 125 «О техническом задании на развитие интегрированной информационной системы Евразийского

экономического союза» // Официальный сайт Евразийского экономического союза [Электронный ресурс]. URL: http://www.eaeunion.org/. – 09.09.2022.

7. Решение Совета Евразийской экономической комиссии от 14.07.2021 N 63 (ред. от 25.11.2022) «О реализации проекта "Цифровое техническое регулирование в рамках Евразийского экономического союза"» // Официальный сайт Евразийского экономического союза [Электронный ресурс]. URL: http://www.eaeunion.org/. – 04.08.2021.
8. Протокол о внесении изменений в Договор о Таможенном кодексе Евразийского экономического союза от 11 апреля 2017 г. (Санкт-Петербург, 25 декабря 2023 г.) (не вступил в силу) // Официальный сайт Евразийского экономического союза [Электронный ресурс]. URL: http://www.eaeunion.org/. – 28.12.2023.
9. Treaty on European Union // OJ C 191, 29.7.1992, p. 1–112
10. Treaty on the Functioning of the European Union // OJ C 326, 26.10.2012, p. 47–390.
11. Charter of Fundamental Rights of the European Union // OJ C 326, 26.10.2012, p. 391–407.
12. 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) // OJ L 119, 4.5.2016, p. 1–88.
13. Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012 // OJ L 347, 28.12.2017, p. 35–80.

14. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union // OJ L 303, 28.11.2018, p. 59–68.
15. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. // OJ L 79I , 21.3.2019, p. 1–14.
16. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // OJ L 151, 7.6.2019, p. 15–69.
17. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services 9 PE/56/2019/REV/1) // OJ L 186, 11.7.2019, p. 57-79.
18. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. PE/28/2021/INIT // OJ L 202, 8.6.2021, p. 1–31.
19. Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (PE/88/2021/REV/2) // OJ L 151, 2.6.2022, p. 1–33.
20. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) PE/30/2022/REV/1 // OJ L 277, 27.10.2022, p. 1–102.

21. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (PE/24/2024/REV/1) // OJ L, 2024/1689, 12.7.2024.
22. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (PE/32/2022/REV/2) // OJ L 333, 27.12.2022, p. 80–152.
23. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) PE/17/2022/REV/1 // OJ L 265, 12.10.2022, p. 1–66.
24. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. PE/54/2022/REV/1 // OJ L 150, 9.6.2023, p. 40–205.
25. Commission Implementing Regulation (EU) 2015/1986 of 11 November 2015 establishing standard forms for the publication of notices in the field of public procurement and repealing Implementing Regulation (EU) No 842/2011 // OJ L 296, 12.11.2015, p. 1–146.
26. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) // OJ L 178, 17.7.2000, p. 1-16.
27. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the

business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC // OJ L 267, 10.10.2009, p. 7–17.

28. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) // OJ L 95, 15.4.2010, p. 1-24.
29. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC // OJ L 94, 28.3.2014, p. 65–242.
30. Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes (recast) // OJ L 173, 12.6.2014, p. 149–178.
31. Directive 2014/55/EU of the European Parliament and of the Council of 16 April 2014 on electronic invoicing in public procurement // OJ L 133, 6.5.2014, p. 1–11.
32. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) // OJ L 173, 12.6.2014, p. 349–496.
33. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) // OJ L 241, 17.9.2015, p. 1–15.
34. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or

the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA // OJ L 119, 4.5.2016, p. 89–131.

35. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // OJ L 194, 19.7.2016, p. 1-30.
36. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (PE/52/2018/REV/1) // OJ L 321, 17.12.2018, p. 36–214.
37. Joint communication to the European Parliament, the Council, the European economic and Social Committee and the Committee of the regions «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace» (JOIN (2013) 1 final). Brussels, 7.2.2013 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 (accessed: 30.05.2022).
38. Joint Communication to the European Parliament and the Council «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU» (JOIN/2017/0450 final) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (accessed: 30.05.2022).
39. Joint communication to the European parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade. JOIN(2020) 18 final. Brussels, 16.12.2020 // [Electronic source]. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (accessed: 19.12.2022).
40. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. COM(2010)245 final.

Brussels, 19.5.2010. [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R%2801%29 (accessed: 19.12.2022).

41. Communication from the Commission to the European parliament, the Council, the European economic and social committee and the Committee of the regions «End-to-end e-procurement to modernize public administration» (COM/2013/0453 final) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0453 (accessed: 30.05.2022).
42. Communication from the Commission to the European Parliament, the European council, the Council, the European economic and social committee and the Committee of the regions: The European Green Deal (COM/2019/640 final). Brussels, 11.12.2019 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN (accessed: 30.05.2022).
43. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A European strategy for data (COM/2020/66 final). Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (accessed: 30.05.2022).
44. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed: 30.05.2022).

45. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: Shaping Europe's digital future (COM/2020/67 final). Brussels, 19.2.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067 (accessed: 19.12.2022).
46. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: A Digital Single Market Strategy for Europe. COM/2015/0192 final. Brussels, 6.5.2015 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 (accessed: 19.12.2022).
47. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises // OJ L 239, 19.9.2017, p. 36–58.

Официальные документы ЕС и ЕАЭС

48. Заявление о цифровой повестке ЕАЭС [Электронный ресурс] // Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Pages/docs.aspx (дата обращения: 14.03.2024).
49. Общие подходы к формированию цифрового пространства Евразийского экономического союза в перспективе до 2030 года (Подготовлено ЕЭК в рамках выработки предложений по формированию цифрового пространства ЕАЭС) [Электронный ресурс] // Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Pages/docs.aspx (дата обращения: 14.03.2024).
50. Memorandum of understanding on online advertising and intellectual property rights (21.06.2018) [Electronic source] // European Commission.

URL: https://ec.europa.eu/docsroom/documents/30226 (accessed: 30.0.2022).

51. The Digital Economy and Society Index [Electronic source] // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 30.05.2022).
52. Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September (2018 COM/2018/630 final). Brussels, 12.9.2018 [Electronic source] // European Commission. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018PC0630 (accessed: 30.05.2022).
53. Europe 2020. A European strategy for smart, sustainable and inclusive growth [Electronic source]. URL: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf (accessed: 19.12.2022).
54. The European Union explained: Digital agenda for Europe [Electronic source]. URL: http://europa.eu/pol/index_en.htm http://europa.eu/!bY34KD (accessed: 19.12.2022).
55. A Europe fit for the digital age [Electronic source] // European Commission. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en (accessed: 19.12.2022).
56. State of the Union Address by President von der Leyen at the European Parliament Plenary [Electronic source] // European Commission. 16 September 2020 . URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (accessed: 19.12.2022).

57. Proposal for a Council directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services. COM/2018/0148 final. Brussels, 21.3.2018 (ongoing) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:148:FIN (accessed: 19.12.2022).
58. Proposal for a Regulation of the European parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. COM/2020/825 final (adopted) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN (accessed: 19.12.2022).
59. Proposal for a Regulation of the European parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). COM/2020/842 final (adopted) // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN (accessed: 19.12.2022).
60. Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. COM/2021/206 final. Brussels, 21.4.2021 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206 (accessed: 19.12.2022).
61. Proposal for a Regulation of the european parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM/2020/593 final. Brussels, 24.9.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593 (accessed: 19.12.2022).
62. Commission report: EU data protection rules empower citizens and are fit for the digital age [Electronic source] // European Commission. 24 June

2020. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018PC0630 (accessed: 20.12.2022).

63. Advice on ‘Initial Coin Offerings and Crypto-Assets. ESMA. 2019.
64. EBA report with advice on crypto-assets, 2019.
65. Proposal for a Regulation of the European parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology. COM/2020/594 final. Brussels, 24.9.2020 // [Electronic source]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594 (дата обращения: 20.12.2022).
66. Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper). European Court of Auditors. 2019.

Материалы судебной практики

67. Order of the President of the General Court of 27 September 2023. Amazon Services Europe Sàrl v European Commission. Case T-367/23 R // ECLI:EU:T:2023:589.
68. Order of the Vice-President of the Court of 27 March 2024. European Commission v Amazon Services Europe Sàrl. Case C-639/23 P(R) // ECLI:EU:C:2024:277.

Диссертации и авторефераты диссертаций

69. Галушко Д.В. Теория и практика правового регулирования интеграционных процессов в свете вызовов Брекзита: дис. … д-ра юрид. наук. – М., 2023. – 544 с.
70. Грибанов Ю.И. Цифровая трансформация социально-экономических систем на основе развития института сервисной интеграции: дис. … д-ра эконом. наук. – СПб., 2019. – 355 с.

71. Марченко А.Ю. Правовой анализ новейшего законодательства ЕС о применении технологий искусственного интеллекта: дис. … канд. юрид. наук. – М., 2022. – 208 с.

Научная литература

72. Боден Ж. Метод легкого познания истории / под ред. М. С. Бобковой. – М.: Наука, 2000. – 411 с.
73. Интеграционное право в современном мире: сравнительно-правовое исследование / ред. С. Ю. Кашкин. – М.: Проспект, 2015. –412 с.
74. Интеграционное правосудие: сущность и перспективы: Монография / С.Ю. Кашкин, П.А. Калиниченко, Я.С. Кожеуров, Е.Г. Моисеев; Отв. ред. С.Ю. Кашкин. – М.: Норма: НИЦ ИНФРА-М, 2019. – 112 с.
75. Клемин А.В. Европейское право и Германия: баланс национального и наднационального. Европейское Сообщество, Германия, право: национальный консерватизм, коллизии и единство. – Казань: Изд-во Казанск. ун-та, 2004. – 588 с.
76. Лифшиц И. М. Международное финансовое право и право Европейского союза: взаимодействие и взаимовлияние: монография. – Москва: Юстицинформ, 2020. – 548 с.
77. Нешатаева Т. Н. Суд и право: евразийская интеграция: монография. – Москва: Норма: ИНФРА-М, 2024. – 336 с.
78. Сонин В.В. Легальность параллельного экспорта товаров с зарегистрированными товарными знаками из КНР в Россию в современных условиях (анализ китайского законодательства и судебной практики). – М., 2023. – 10 с.
79. Уэбстер Ф. Теории информационного общества / Под ред. Е. Л. Вартановой. – М.: Аспект Пресс, 2004. – 400 с.
80. Цифровая повестка и инициативы в области цифровых технологий в условиях COVID-19 (обзор практик Европейского союза, Организации

экономического сотрудничества и развития, а также других стран). – М.: НИУ ВШЭ, 2020. – 19 с.

81. Энтин М.Л., Энтина Е.Г. Политическое и регуляторное обеспечение мировых интеграционных процессов: Усилия России, Китая, Индии, ЕС и США по обретению стратегической глубины в 2022–2023 годах: Научная монография / М.Л. Энтин, Е.Г. Энтина. – Москва: Галактика, Издательский Дом «Зебра Е», 2023. – 622 с.
82. Agamben G. Homo Sacer. Sovereign Power and Bare Life. – Stanford: Stanford University Press, 1998. – 217 p.
83. Creemers R. China’s Conception of Cyber Sovereignty / in: D. Broeders & B. Berg (Eds.), Governing Cyberspace: Behavior, Power and Diplomacy. – Rowman&Littlefield, 2020. – 34 p.
84. Dickinson I. The quest for a fair price in the digital world - Frand in the DMA 2022. Frontier Economics. – United Kingdom, 2022. – 6 p.
85. Falk R. Sovereignty. The Oxford Companion to Politics of the World. – New York, Oxford, 1993. – 1018 p.
86. Heldt A. EU Digital Services Act: The White Hope of Intermediary Regulation // in: Digital Platform Regulation. Global Perspectives on Internet Governance / T. Flew, F.R. Martin (eds). – Palgrave Macmillan, 2022. – P. 69-84.
87. Mueller M. Will the internet fragment? Sovereignty, globalization and cyberspace. – Polity, 2017. – 140 p.
88. Outhwaite W., Ray L. Social Theory and Postcommunism. – Oxford: Balckwell, 2005. – 272 p.
89. The Platform Economy. Designing a Supranational Legal Framework / Editors: M.I. Inozemtsev, E.L. Sidorenko, Z.I. Khisamova. – Palgrave Macmillan Singapore, 2022. – 455 p.
90. Westeren K.I. Foundations of the knowledge economy: innovation, learning, and clusters. – Cheltenham, UK: Edward Elgar. 2012. – 296 p.

Учебная литература

91. Бирюков М.М., Энтин Л.М., Энтин М.Л. Европейское право. Основы интеграционного права Европейского Союза. – М.: Норма, 2023. – 528 с.
92. Европейское международное право: Учебник / Ю.М. Колосов, Э.С. Кривчикова, Д.В. Иванов и др.; Отв. ред. Ю.М. Колосов, Э.С. Кривчикова, П.В. Саваськов. – М.: Международные отношения, 2005. – 408 с.
93. Европейское право. Основы интеграционного права Европейского союза и Евразийского экономического союза: учебник / рук. авт. кол. и отв. ред. Л.М. Энтин, М.Л. Энтин. – М.: Норма: ИНФРАМ, 2018. – 528 с.
94. Европейское право. Отрасли права Европейского Союза и Евразийского экономического союза: учебник / рук. авт. кол. и отв. ред. Л.М. Энтин, М.Л. Энтин. – М.: ИНФРА-М, 2023. – 416 с.
95. Кашкин С. Ю. Право Европейского союза в 2 т. / С. Ю. Кашкин, А. О. Четвериков; отв. ред. С. Ю. Кашкин. – 4-е изд., перераб. и доп. – М.: Юрайт, 2024. – 1647 с.
96. Курс международного права: Международно-правовые формы интеграционных процессов в современном мире. В 7-ми томах. Т. 7 / Бардина М.П., Войтович С.А., Колосов Ю.М., Кузнецов В.И., и др.; Отв. ред.: Усенко Е.Т. – М.: Наука, 1993. – 328 с.
97. Право Европейского союза в 2 ч. / А. Х. Абашидзе [и др.]; под редакцией А. Х. Абашидзе, А. О. Иншаковой. 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 892 с.
98. Право Европейского союза: учебник для вузов / А. Я. Капустин [и др.]. – Москва: Издательство Юрайт, 2022. – 387 с.

Публикации в периодических изданиях

99. Бороздин А.Н., Коварда В.В. Анализ системы обеспечения защиты информации в процессе цифровизации ее оборота в рамках ЕАЭС в аспекте повышения экономической безопасности // Вестник Евразийской науки. – 2020. – Т. 12. № 4. – С. 1-15.
100. Буткевич С. А. Фейк-ньюс и медиа: проблемы дифференциации и пенализации // Юристъ-Правоведъ. – 2021. – № 2(97). – С. 74-79.
101. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. – 2016. – № 6(51). – С. 76-91.
102. Винник Д.В. Цифровой суверенитет: политические и правовые режимы фильтрации данных // Философия науки. – 2014. – № 2 (61). – С. 95-113.
103. Войников В. В., Энтина Е. Г., Энтин М. Л. Перспективы, потребности и подводные камни конституционализации ЕС и ЕАЭС // Полис. Политические исследования. – 2019. – № 4. – С. 89-103.
104. Войников В.В. Право Европейского Союза в практике Европейского Суда по правам человека // Международное правосудие. – 2020. – №1 (33). – С. 50–66.
105. Войников В.В. Правовое регулирование информационных систем пространства свободы, безопасности и правосудия ЕС // Вестник Саратовской государственной юридической академии. – 2019. – № 4 (129). – С. 99-111.
106. Гедгафов М. М. Развитие кибертерроризма в условиях глобализации информационного пространства // Образование и право. – 2021. – № 6. – С. 304-308.
107. Гончаренко Л.С. Цифровая экономика как фактор социально-экономической трансформации России // Вестник ЧелГУ. – 2019. – №3 (425). – С. 43-49.

108. Егорова Е.Н. Перспективы перехода европейского союза к политическому союзу: договор, учреждающий конституцию для Европы // Идеи конституционализма в юридической науке: история и современность. Сборник материалов третьей международной научной конференции, посвященной памяти профессора В.М.Курицына. – 2019. – С. 67-81.
109. Ермак К.А. Информационная безопасность как элемент интеграции в рамках ЕАЭС // Социальные новации и социальные науки. – 2023. – №3 (12). – С. 132-142.
110. Зиновьева Е., Булва В. Цифровой суверенитет ЕС // Современная Европа. – 2021. – №2. – С. 40-49.
111. Зиновьева Е.С. Проблемы международного управления Интернетом в контексте цифрового суверенитета // Международная жизнь. – 2020. – Специальный выпуск. – С. 133-137.
112. Зуева А.М., Шайдуллова М.В. Цифровой транспортный коридор как новый элемент в организации таможенного контроля // NovaUm.Ru. – 2018. – № 13. – С. 99–101.
113. Иванова О.Б., Хапилин А.Ф., Хапилин С.А. Цифровая повестка ЕАЭС в контексте модернизации системы таможенного администрирования // Вестник Ростовского государственного экономического университета (РИНХ). – 2020. – № 1 (69). – С. 157-163.
114. Игумнова Л.О. Образ нормативной силы Евросоюза в заявлениях Европейской внешнеполитической службы // Современная Европа. – 2017. – № 6 (78). – С. 81-93.
115. Касьянов Р. А. Международный опыт противодействия киберугрозам / Р. А. Касьянов // Российский следователь. – 2023. – № 6. – С. 59-63.
116. Касьянов Р.А. Обеспечение экономических прав и свобод человека и построение единого рынка финансовых услуг в Европейском союзе //

Вопросы российского и международного права. – 2019. – Т. 9. № 4. – С. 152-161.

117. Касьянов, Р. А. Правовые основания цифровизации финансового сектора Европейского союза // Банковское право. – 2023. – № 2. – С. 49-58.
118. Касьянов, Р. А. Цифровизация как важный фактор регулирования российского финансового рынка и Союза рынков капитала ЕС / Р. А. Касьянов, М. А. Евдокимов // Право и цифровая экономика. – 2022. – № 4(18). – С. 36-47.
119. Касьянов, Р. А., Пучкова, А. П. (2022). Правовое регулирование государственных закупок в ЕС и ЕАЭС: тенденции к цифровизации // Цифровое право. – 2022. – № 3(2). – С. 51–68.
120. Колосов Ю.М. О понятии европейского международного права // Российский ежегодник международного права. – 2006. – С. 194-198.
121. Кольцов А.Н. О глобализации и суверенитете государств // Вестник Чувашского университета. – 2004. – № 1. – С. 50-53.
122. Копылов В. А. Защита интеллектуальной собственности в сети интернет на современном этапе развития гражданского оборота // Будущее науки-2020: сборник научных статей 8-й Международной молодежной научной конференции: в 5 томах, Курск, 21–22 апреля 2020 года. – Курск: Юго-Западный государственный университет, 2020. – С. 281-287.
123. Кошелева О.Э., Воробьева М.Д. Параллельный импорт в качестве антисанкционной меры // Бюллетень информационных технологий. – 2023. – №1 (25). – С. 39-44.
124. Кузякин Ю.П., Мухин А.И. Цифровая трансформация таможенного контроля: состояние и перспективы // Юридическая наука. – 2023. – №8. – С. 111-117.

125. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. – 2014. – №9. – С. 8-15.
126. Ларионова С. Л. Методика защиты персональных данных с учетом требований регламента ЕС General Data Protection Regulation // Инновации и инвестиции. – 2020. – № 6. – С. 198-205.
127. Литвинова Т. Н. Европейская и российская политики противодействия кибертерроризму (на примере борьбы с «кибер-джихадом») // Национальная безопасность / nota bene. – 2020. – № 3. – С. 32-47.
128. Лифшиц И. М. Проблема квалификации права Европейского Союза как правовой системы // Актуальные проблемы российского права. – 2019. – №11 (108). – С. 153-162.
129. Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. – 2022. – № 1. – С. 61–75 .
130. Лю К.А. Основные направления наднационального регулирования общественных отношений в цифровой сфере на современном этапе (на примере Европейского союза) // Международное право и международные организации / International Law and International Organizations. – 2023. – № 1. – С. 12–25 .
131. Лю К.А. Новый порядок регулирования внешней электронной торговли в ЕАЭС: новеллы таможенного законодательства // Инновации и инвестиции. – 2024. – № 2. – С. 69–74 .
132. Лю К.А. Основные направления международно-правового и наднационального регулирования цифрового пространства в рамках ЕАЭС на современном этапе // Право и управление. XXI век. – 2024. – Т. 20. № 1. – С. 84–91 .
133. Мозер С.В., Секербаева Д.К. К вопросу о функционировании тематического блока «электронная таможня» в Евразийском

экономическом союзе // Социально-политические науки. – 2020. – Т. 10. № 1. – С. 49-59.

134. Мостовой Г. И. «Цифровой тупик» защиты интеллектуальной собственности в сети интернет и возможности его преодоления / Г. И. Мостовой, В. И. Харин // Вопросы российской юстиции. – 2020. – № 8. – С. 576-584.
135. Нешатаева Т. Н. Интеграция и наднационализм // Вестник Пермского университета. Юридические науки. – 2014. – №2 (24). – С. 243-248.
136. Оюн Ч. О., Попантонопуло Е. В. Объекты критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. – 2018. – №9. – С. 45-49.
137. Попова И.М. Проблемы реализации цифровой повестки ЕАЭС // Вестник международных организаций: образование, наука, новая экономика. – 2021. – №1. – С. 127-141.
138. Ревина С.Н., Лунева У.С. Вопросы таможенного регулирования в условиях развития интернет-торговли // МНИЖ. – 2023. – №4 (130). – С. 1-5.
139. Саворская Е.В. Сущность концепции «Нормативной силы» Европейского союза // Балт. рег. – 2015. – №4. – С. 90-104.
140. Самарин А.А. Право и экстерриториальность в условиях глобализации // Вестник Саратовской государственной юридической академии. – 2015. – № 1 (102). – С. 115-124.
141. Саркисян Т.С. Интеграционный "План ГОЭЛРО" для XXI века // Россия в глобальной политике. – 2021. – №3 (109). – С. 136-149.
142. Степанян А.Ж. Регламент Европейского Союза об искусственном интеллекте (Artificial Intelligence Act): первый взгляд на проект // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2021. – № 7. – С. 93-98.

143. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. – 2018. – № 2 (254). – С. 5-17.
144. Толстых В.Л. Размышления о евразийской интеграции // Sumus ubi sumus. Международное право XXI века: мир и безопасность, сотрудничество, права человека. Liber amicorum в честь профессора Л.П. Ануфриевой. – М.: Проспект, 2016. – С. 277-279.
145. Фельдман П. Я. «Постправда» и «фейк-ньюз» в современном коммуникационном пространстве: перспективы политико-правового регулирования // Гражданин. Выборы. Власть. – 2019. – № 2(12). – С. 134-146.
146. Филиппов А. Суверенитет // Апология. – 2005. – № 3. – С. 58-67.
147. Хиршлер М., Цимерман Б. Западно-европейские интеграционные объединения. Право: пер. с нем. / под общ. ред. и предисл. Э. М. Аметистова, М. И. Брагинского. – М., 1987. – С. 75-77.
148. Хлопов О. А. Проблемы кибербезопасности и защиты критической инфраструктуры // The Scientific Heritage. – 2020. – № 45-5(45). – С. 64-69.
149. Чубукова С. Г. Правовые проблемы обработки персональных данных в контексте COVID-19: опыт России и ЕС // Роль и значение права в условиях пандемии: Монография по итогам Международного онлайн-симпозиума / Под общей редакцией В.В. Блажеева, М. А. Егоровой. – Москва: Общество с ограниченной ответственностью "Проспект", 2021. – С. 52-62.
150. Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Сибирское юридическое обозрение. – 2019. – №1. – С. 29-35.

151. Шалаевская В. Н. Антимонопольное право в эпоху цифровой экономики // Умная цифровая экономика. – 2022. – Т. 2. № 1. – С. 31-36.
152. Шаститко А.Е., Шпакова А.А. Регулирование трансграничного электронного документооборота в Евразийском экономическом союзе // Государственное управление. Электронный вестник. – 2018. – № 71. – С. 242-269.
153. Шафоростова К. И. Защита интеллектуальной собственности в сети Интернет на национальном и международно-правовом уровне // Научно-методический электронный журнал Концепт. – 2019. – № 6. – С. 161-166.
154. Энтин М.Л. Перспективы, потребности и подводные камни конституционализации ЕС и ЕАЭС / М.Л. Энтин, Е.Г. Энтина, В.В. Войников // Полис. Политические исследования. – 2019. – № 4. – С. 89-103.
155. Энтин М.Л., Войников В.В., Торкунова Е.А. Новый этап в институционально-правовом обустройстве пространства свободы, безопасности и правосудия ЕС // Московский журнал международного права. – 2018. – № 2. – С. 102-114.
156. Энтин М.Л., Энтина Е.Г., Торкунова Е.А. Сегодня и завтра ЕС сквозь призму правового инструментария углубления интеграции. Часть I // Современная Европа. – 2019. – №1. – С. 27-37.
157. Энтин М.Л., Энтина Е.Г., Торкунова Е.А. Сегодня и завтра ЕС сквозь призму правового инструментария углубления интеграции. Часть II // Современная Европа. – 2019. – № 2. – С. 39-49.
158. Aaronson S. A. The digital trade imbalance and its implications for internet governance // Centre for International Governance Innovation: Working Paper №25/2016. – 40 p.

159. Andriychuk O. Do DMA obligations for gatekeepers create entitlements for business users? // Journal of Antitrust Enforcement. – 2023. – Vol. 11. Is. 1. – P. 123–132.
160. Chiarella M.L. Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment // Athens Journal of Law. – 2022. – № 9. – P. 1-25.
161. Church P., Pehlivan C.N. The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability // Global Privacy Law Review. – 2023. – Vol. 4. Is. 1. – P. 53-59.
162. Colangelo G. DMA begins // Journal of Antitrust Enforcement. – 2023. – Vol. 11. Is. 1. – P. 116–122.
163. Couture S., Toupin S. What does the notion of «sovereignty» mean when referring to the digital? // New Media & Society. – 2019. – № 21(10). – P. 2305-2322.
164. Daems I. The complexity and practical challenges of implementing the new DMA // Competition Law & Policy Debate. – 2022. – № 7(3). – P. 106-112.
165. Davola A., Malgieri G. Data, Power and Competition Law: The (Im)Possible Mission of the DMA? // Research in Law and Economics. – 2023. – Vol. 31. – P. 53-74.
166. Entin M.L. Difficult Choice of a Rational Approach to Regulating the Activities of Digital Platforms / M.L.Entin, E.A.Torkunova, S.O.Korogod // The Platform Economy. – Palgrave Macmillan, Singapore, 2022. – P. 253–269.
167. Ferracane M. Restrictions on Cross-Border Data Flows: A Taxonomy // European Centre for International Political Economy: Working Paper №1/2017. – 27 p.
168. Gallagher N., Abecasis P. The DMA and the role of economics // Competition Law & Policy Debate. – 2022. – № 7(3). – P. 113-120.

169. Grant P. Technological sovereignty: forgotten factor in the «hitech» razzamatazz // Prometheus. – 1982. – T. 1. № 2. – P. 239-270.
170. Greater Eurasia: In Search of a Legal Order / У.Э. Батлер, М.Л. Энтин, Е.Г. Энтина, Е.А. Торкунова / Полис. Политические исследования. – 2020. – №4. – С. 9-23.
171. Hoffmann J., Herrmann L., Kestler L. Gatekeeper's Potential Privilege – the Need to Limit DMA Centralisation // Journal of Antitrust Enforcement. – Vol. 12. Is. 1. – P. 126-147.
172. Hustad E., Olsen D. Creating a sustainable digital infrastructure: The role of service-oriented architecture. – 2020. – P. 597-604.
173. Kelly E. Decoding Europe’s new fascination with «tech sovereignty» // Science/Business. – 2020. – № 9. [Электронный ресурс]. Режим доступа: https://sciencebusiness.net/news/decoding-europes-new-fascination-tech-sovereignty (дата обращения: 07.11.2024).
174. Kennedy P., Messner D. Global Trends and Global Governance. Sterling // Pluto Press. – 2002. – P. 143-144.
175. Madiega T. Digital sovereignty for Europe // European Parliamentary Research Service (EPRS) Ideas Paper. – 2020. – 12 p.
176. Marchart O. The Other Side of Order: Towards a Political Theory of Terror and Dislocation // Parallax. – 2003. – Vol. 9. № 1. – P. 102-111.
177. O’Neill B. Broadcast Sovereignty in a Digital Environment. – Dublin Institute of Technology, 2006. – P. 179-197.
178. Or B., Magali E. Who should guard the gatekeepers: does the DMA replicate the unworkable test of Regulation 1/2003 to settle conflicts between EU and national laws? // CPI Antitrust Chronicle. – 2022. – № 12. – P. 37-42.
179. Schöning F., von Schreitter F. Showcases and showstoppers: the DMA’s impact on merger control in digital markets // Competition Law & Policy Debate. – 2022. – № 7(3). – P. 121-129.

180. Sørensen G. Sovereignty: Change and Continuity in a Fundamental Institution // Political Studies. – 1999. – Vol. XLVII. – P. 590–604.
181. Staab P., SieronS., Piétron D. Counter-Hegemonic Neoliberalism: Making Sense of EU Platform Regulation // Weizenbaum Journal of the Digital Society. – 2022. – № 2(1). – P. 1-18.
182. Tréguer F. Intelligence reform and the Snowden paradox: The case of France // Media and Communication. – 2017. – № 5 (1). – P. 17–28.

Электронные ресурсы

183. Британия оставит российский процессор без технологий // Lenta.ru. 5 мая 2022 г. [Электронный ресурс]. Режим доступа: https://lenta.ru/news/2022/05/05/buy/ (дата обращения: 03.02.2024).
184. В ЕАЭС продолжается создание экосистемы цифровых транспортных коридоров // ЕЭК: официальный сайт. 12.12.2022. [Электронный ресурс]. Режим доступа: https://eec.eaeunion.org/news/v-eaes-prodolzhaetsya-sozdanie-ekosistemy-tsifrovykh-transportnykh-koridorov/ (дата обращения: 01.02.2024).
185. Дмитрий Вольвач: страны ЕАЭС готовят соглашение по борьбе с нарушениями прав на интеллектуальную собственность в Интернете // Минэкономразвития: официальный сайт. 08.12.2023. [Электронный ресурс]. Режим доступа: https://www.economy.gov.ru/material/news/dmitriy_volvach_strany_eaes_gotovyat_soglashenie_po_borbe_s_narusheniyami_prav_na_intellektualnuyu_sobstvennost_v_internete.html (дата обращения: 01.02.2024).
186. Какие микропроцессоры разрабатывают в России? И что с ними будет из-за санкций? // ТАСС. 10 июня 2022 г. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/14868777 (дата обращения: 03.02.2024).

187. Министр ЕЭК Карине Минасян в интервью CNews – об общих цифровых экосистемах Армении, Белоруссии, Казахстана, Кыргызстана и России // ЕЭК: официальный сайт. [Электронный ресурс]. Режим доступа: https://eec.eaeunion.org/news/speech/15-01-2020-1/ (дата обращения: 31.01.2024).
188. Мишустин назвал Россию «чемпионом мира» по числу введенных против нее санкций // ТАСС. 15 марта 2023 г. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/17274023 (дата обращения: 03.02.2024).
189. Проект «Работа без границ» стартовал в ЕАЭС // ЕЭК: официальный сайт. 01.07.2021. [Электронный ресурс]. Режим доступа: https://eec.eaeunion.org/news/proekt-rabota-bez-granic-startoval-v-eaes/ (дата обращения: 01.02.2024).
190. Сарханянц К. Еврокомиссия стирает границы в онлайне [Электронный ресурс] // Режим доступа: http://www.kommersant.ru/doc/2723377 (дата обращения: 19.12.2022).
191. Gérot M., Maxwell W. Will the GDPR frustrate Europe’s plans for AI? [Electronic source] // ItProPortal. March 18, 2020. URL: https://www.itproportal.com/features/will-the-gdpr-frustrate-europes-plans-for-ai/ (accessed: 19.12.2022).