Зарубежный опыт. Международное сотрудничество

ЦИФРОВОЕ ПРОСТРАНСТВО: ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ В ЕВРОАТЛАНТИЧЕСКИХ СТРАНАХ

Статья рекомендована к публикации главным редактором Т. В. Ершовой 05.09.2025.

Татунц Светлана Ахундовна

Доктор социологических наук, кандидат исторических наук, профессор
Московский государственный университет им. М. В. Ломоносова
Факультет мировой политики
Профессор
Москва, Российская Федерация
S.Tatunts@fmp.msu.ru

Аннотация

Регулирование цифрового пространства не знает границ и является приоритетным ввиду скорости технологического развития. В статье автор анализирует опыт стран ЕС, Великобритании и США, в т.ч. по вопросам регулирования работы ИИ и связанным с ними угрозами. Подробно исследуется европейское законодательство и практика правоприменения. На теоретическом уровне сравниваются модели регулирования ЕС, США и КНР, в корне отличающиеся в целеполагании и этических принципах. Делается вывод о высокой эффективности европейской системы регулирования (GDPR, DSA, DMA, EU AI Act, включая британские аналоги), и разрозненности регионального законодательства на уровне штатов при полном отсутствии федерального законодательства по регулированию цифрового пространства в США. В рамках полипарадигмального метолодогического подхода на конкретных примерах цифровой экономики обосновывается необходимость скорейшей доработки законодательств во всех исследуемых странах.

Ключевые слова

регулирование; цифровое пространство; защита данных; ИИ; GDPR; DSA; DMA

Введение

Уже много десятилетий существует широкий консенсус по поводу того, что не всё, что технически возможно, является социально желательным. Именно поэтому регулирование цифрового пространства, окружающее нас повседневно, приобретает особую значимость. Необходимость принятия государственных мер контроля и надзора над цифровыми услугами и связанными с ними правами граждан имеется во всех странах мира, и сегодняшние принципиальные подходы правительств к надзору за онлайн-платформами, поисковыми системами и интернет-инфраструктурой нацелены, в первую очередь, на защиту потребителей, предотвращение образования монополий на рынке и на обеспечение безопасной, прозрачной и конкурентоспособной цифровой среды.

Учитывая, что в российском научном дискурсе пока преобладают такие узкоспециальные темы, как борьба за цифровой суверенитет, регулирование цифровой экономики в целом и цифровых финансовых активов в частности или правовое обеспечение маркетплейсов, в настоящей статье ставится более широкая **цель**, — рассмотреть историю создания, практику применения и эффективность правового регулирования всего цифрового пространства, включая и цифровую экономику, и соцсети, и медиапространство, и применение искусственного интеллекта (ИИ) в евроатлантических странах.

Автор исследует набор имеющихся там на национальном и наднациональном уровне законов. На конкретных примерах цифровой экономики различных стран рассматривается вопрос,

© Татунц С. А., 2026.
Производство и хостинг журнала «Информационное общество» осуществляется Институтом развития информационного общества.
Данная статья распространяется на условиях международной лицензии Creative Commons «Атрибуция — Некоммерческое использование — На тех же условиях» Всемирная 4.0 (Creative Commons Attribution — NonCommercial — ShareAlike 4.0 International; CC BY-NC-SA 4.0). См. https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.ru
https://doi.org/10.52605/16059921_2026_05_172

в какой степени существующее законодательство на практике действительно работает. Следует понять, как удается или не удается законодателям изучаемых стран посредством регулирования выдержать в цифровом пространстве равновесие между защитой свободы слова граждан и предотвращением дезинформации; между правами человека и нормативным контролем государства; и получается ли у них не допускать в своих странах распространение дезинформации через цифровую среду для разжигания ненависти и организации беспорядков [3, с. 20].

Для этого автор ставит следующие **задачи**:

- проанализировать основные законодательные и подзаконные акты, регулирующие цифровое пространство в евроатлантических странах;
- оценить их эффективность или неэффективность и действенность предусмотренных санкций в случае их нарушения;
- подвергнуть сравнительному анализу регулирование цифрового пространства в англосаксонских государствах и в странах ЕС;
- выявить изъяны существующего регулирования.

Выбор евроатлантических стран обусловлен большими различиями в подходах к законодательству в цифровом пространстве. В то время как США и Великобритания придерживаются крайне либерального подхода, Евросоюз принял самые строгие нормы регулирования цифрового пространства.

Автором в рамках **полипарадигмального методологического подхода** используются системно-структурный и сравнительно-правовой методы, общетеоретические, а также эмпирические методы исследования.

Правовое регулирование цифрового пространства исключительно важно для всех стран мира, в т. ч. в связи с возникающими угрозами кибер-терроризма, если отнестись ответственно к возможностям современных средств ИИ за минуты разработать хакерские атаки на критическую инфраструктуру (тест фирмы Anthropic в августе 2026 г. показал, как Claude Mythos стал вышедшим из-под контроля хакером).

Сегодня исследователи отмечают высокие темпы развития цифрового пространства, дизруптивное (подрывающее) значение все новых и новых цифровых продуктов для буквально всех секторов экономики и сфер жизни человека, и существование «мира цифры» вне привычных геополитических границ, что является самым серьезным вызовом для национальных и наднациональных регуляторов. Как отмечают российские эксперты, регулирование в отношении «цифры» всегда находится в «догоняющем» положении, и есть опасность излишнего «зарегулирования» отрасли, которое может затормозить ее развитие [1, с. 129].

Огромные объемы передаваемых данных приводят к постоянно растущему разделению труда, и, как опасаются немецкие исследователи, к неконтролируемому сбору больших объемов персональных данных в сочетании с интеллектуальным анализом и, в конечном итоге, — к тотальной «прозрачности граждан» [9, с. 1–3].

Свою (отрицательную) «лепту» внесла пандемия COVID-19, когда власти всех стран, в т.ч. западных, получили больший доступ к личным данным, и заметно снизилась чувствительность граждан к нарушению границ их частной жизни ради безопасности общества в целом [2, с. 161].

На более теоретическом уровне ясно, что **Европейский союз** при регулировании цифрового пространства в целом придерживается **принципиального подхода**, **основанного на правах человека и защите его данных**. Эта модель контрастирует с подходами, практикуемыми в **США**, — созданием максимально эффективных решений и применением их для извлечения выгоды частных фирм. В ней реклама и «умная» привязка клиентов к услугам создают систему **surveillance capitalism** (капитализм слежки). Технологически также успешны интернет-гиганты Китая, создающие в **КНР** другую модель — **surveillance communism** (коммунизм слежки). Американская модель формируется интересами крупных интернет-гигантов, во всех сферах контролирующих обработку данных граждан и стремящихся к максимизации прибыли для финансирования своих чрезвычайно мощных и инновационных интернет-сервисов. Китайская модель также ориентирована на прибыль и имеет государственно-капиталистическую направленность, но одновременно преследует интересы государственной слежки за населением. Тем самым она несовместима с европейскими представлениями о верховенстве права и человеческих ценностях.

1 Общие принципы цифрового регулирования в странах ЕС

Наиболее всеобъемлющим законодательством по регулированию цифровых услуг и цифрового пространства можно считать законодательный пакет Европейского союза. Его фундамент заложен еще в 1970-е гг. (первый закон о защите данных в ФРГ датируется 1977 г.), начиная именно с темы защиты личных данных граждан. В отличие от этого, Северная Америка и некоторые страны Восточной Европы включили эти вопросы в свое законодательство только в 2010-е гг. Так, например, Закон о защите персональных данных в Польше был принят только в 2018 г., после принятия европейского Общего регламента по этому вопросу GDPR, а о США см. ниже.

Как и во многих других вопросах, локомотивом европейского законодательства по вопросам регулирования цифрового пространства выступает Германия, чей национальный **«Закон о защите данных»** (Datenschutzgrundverordnung, DSGVO, 2016 г.) [17] лег в основу европейского «**Общего регламента по защите данных»** (General Data Protection Regulation, **GDPR**, тот же год, но вступил в силу только в 2018 г.).

В статье 5 Европейского регламента по защите данных (GDPR) законодательно закреплены следующие шесть базовых принципов:

- законность, добросовестность, прозрачность: данные могут обрабатываться только при наличии законного разрешения, и пользователи должны четко понимать, что происходит с их данными;
- целевое использование: данные собираются только для оговоренных целей; иное использование в принципе не допускается;
- минимизация данных: обрабатываются только те персональные данные, что необходимы для достижения соответствующей цели;
- точность: данные должны быть объективно верными и актуальными; неактуальные данные должны немедленно удаляться;
- ограничение срока хранения данных с последующим удалением;
- конфиденциальность: данные должны быть защищены от несанкционированной обработки, потери или уничтожения.

Эти принципы стали основой регулирования цифрового пространства в Европейском союзе и создали европейский базовый стандарт, регулирующий сбор, обработку и хранение персональных данных граждан ЕС. Будучи регламентом ЕС (а не директивой), GDPR имеет прямую юридическую силу и не требует имплементации в национальное законодательство. Однако, он предоставляет каждой стране возможность вносить свои изменения [13].

Такая прочная база регулирования была значительно расширена после принятия **«Европейской декларации о цифровых правах и принципах** цифрового десятилетия» (EDDRP) в 2022 г., в которой сделали обязательными к соблюдению любого ведомства, учреждения, компании и организации в ЕС еще другие важные принципы законодательного регулирования цифрового пространства. Все страны-члены ЕС обязаны закрепить их в национальных законах:

- приоритет прав человека (неприкосновенность частной жизни, защита данных);
- технологическая нейтральность (нет привязки к конкретной технологии);
- фокусирование не на самой технологии, а на исходящих от нее рисках, более строгие требования для очень крупных онлайн-платформ и -сервисов (VLOP, VLOSE);
- гармонизация на наднациональном уровне во избежание фрагментации;
- прозрачность и подотчётность, например раскрытие логики алгоритмов, роль крупных фирм как «привратников» («gatekeepers»), дающих шанс малым и средним конкурентам;
- баланс интересов между пользователями, бизнесом и задачами государства, — во имя защиты как граждан, так и бизнеса, и целях сохранения здоровой конкуренции и инновации;
- инклюзивность, т. е. доступность цифрового пространства для людей с ограниченными возможностями, для молодых людей) [7, главы 1-3].

В области ИИ «Европейский Закон об искусственном интеллекте» **(EU Artificial Intelligence Act,** 2024 г.,) является первым в мире комплексным нормативным актом, где все генеративные модели ИИ делятся на три категории риска: недопустимую, высокую и низкую. Согласно закону, приложения и системы недопустимого риска, как например, системы государственные социального рейтинга, применяемые в КНР, запрещены. К приложениям с высоким уровнем риска предъявляются особые юридические требования, например к автоматическому ИИ-отбору

соискателей на вакансии. Остальные приложения низкого риска остаются (пока) нерегулируемыми в ЕС [6].

2 Законодательная практика регулирования в странах ЕС

Основополагающим законодательным актом по регулированию цифрового пространства европейских стран и сердцевиной «Цифровой стратегии для Европы» является Закон о цифровых услугах (**Digital Service Act, DSA)**, принятый в 2022 г. Он направлен на создание безопасной, предсказуемой и заслуживающей доверия онлайн-среды путем установления гармонизированных требований к предоставлению посреднических услуг на едином рынке ЕС [14].

DSA устанавливает, в частности, обязательства по надлежащей осмотрительности и прозрачности для поставщиков посреднических услуг, включая, обязательство создать контактные пункты для органов власти и граждан, а также правила об ответственности и обязательство поставщиков услуг хостинга создать механизмы уведомления и реагирования в отношении незаконного контента. Этот закон обязывает платформы оперативно удалять незаконный контент, обеспечивает защиту несовершеннолетних, запрещает манипулятивные «темные паттерны» и обеспечивает прозрачность в сфере таргетированной рекламы и модерации контента [18].

Второй важнейший закон, регулирующий европейское цифровое пространство, это Закон о конкурентных и справедливых рынках в цифровом секторе (коротко — **Digital Markets Act, DMA,** 2022), который направлен на крупные цифровые платформы (поисковые системы, социальные сети и приложения онлайн-продаж). Он запрещает так называемым «цифровым привратникам» (gate keepers) — крупным IT-компаниям как Google, Amazon и т. д., являющимся квази-монополистами, и поставляющим пользователям непосредственно свои цифровые, — поставить вперед собственные приложения. Также он предписывает обеспечение совместимости мессенджеров для содействия более честной конкуренции. Таким образом, их деятельность фактически регулируется по аналогии с естественными монополиями, и это защищает права малых и средних предприятий на рынке цифровых услуг [15].

Еще один важный закон для регулирования цифрового пространства в ЕС, это Закон о киберустойчивости (**Cyber Resilience Act, CRA**, 2024 г.). В нем устанавливаются общие стандарты кибер-безопасности для аппаратных и программных продуктов с цифровыми элементами, возлагая на их производителей ответственность за безопасность их устройств на протяжении всего их жизненного цикла.

Комплементарное значение во всем этом комплексе европейского цифрового регулирования имеет **Единый регламент электронной идентификации и доверенных услугах (eIDAS,** принят в 2016 г.), который в ЕС определяет правовую базу для надежной электронной идентификации, подписей и печатей, тем самым он прокладывает путь для трансграничных цифровых кошельков идентичности, беспрепятственных платежей.

Надо отметить, что упомянутые выше «Закон о цифровых услугах» (DSA) и «Общий регламент по защите данных» (GDPR) в Европе приводят к относительной ц**ентрализации полномочий** по государственному контролю за цифровым пространством **в руках Еврокомиссии,** оттесняя на второй план гражданское общество и фактически исключая возможность ведения их представителями большинства стратегических судебных процессов в сфере государственного контроля за цифровыми услугами. В этом состоит один из аргументов **оппонентов цифрового законодательства в ЕС.** Так, например, в феврале 2026 г. лидер французской евроскептической **Партии патриотов** (Les Patriotes) Ф. Филиппо, организовал массовые протесты в Париже против закона DSA, опасаясь этого мощного инструмента цензуры и требуя беспрепятственной свободы слова в Интернете и сохранения открытой дискуссии и альтернативных СМИ [11].

Общеевропейский регламент по защите данных, предоставляющий физическим лицам право на доступ, исправление и удаление своих персональных данных — это тот закон, чьи **требования чаще всего нарушаются интернет-гигантами США** в Европе, — и таким образом постоянно попираются права миллионов людей в Евросоюзе.

На этом фоне незначительны те штрафы, что фирмы Google, X, Meta* (*все запрещенные на территории РФ) и др. выплатили после проигранных в Европе судебных тяжб. В основном они были связаны с **нарушением законов о прозрачности рекламы** и непредоставлении исследователям **доступа к открытым данным**. А платформу «X*» И. Маска в декабре 2025 г. оштрафовали на 120 млн. долларов США за ту известную «синюю галочку» для обозначения «проверенных аккаунтов»,

которая вводит пользователей в заблуждение. Ведь в соцсети «X*» можно просто заплатить за статус «проверенного», что затрудняет верно оценить подлинность контента [5].

Это было первое и пока единственное решение Еврокомиссии по нарушению положений DSA за целых 4 года. Далее Еврокомиссия пока только «предварительно установила» (хотя это общеизвестно уже много лет), что Meta*, нарушает DSA тем, что допускает к своим сервисам Instagram* и Facebook* **несовершеннолетних в возрасте до 13 лет**. За это согласно ст. 59 и 60 DSA суды могут вынести намного более суровые наказания (денежные штрафы до 6% от годового оборота фирмы). Но если так долго тянут с таким очевидным решением, то закон плохо работает. В конце концов его слабость еще в том, что большинство его требований **применяются только и крупным онлайн-платформам (VLOP),** имеющим более 45 миллионов активных пользователей в месяц в ЕС, что соответствует 10 % населения ЕС, но их не так уж много (всего 20-30 во всем мире).

3 Регулирование сферы цифровых услуг в Великобритании и США

Если исходить из того, что европейский Закон о цифровых услугах (DSA), по крайней мере частично, создал некий глобальный режим прозрачности регулирования цифрового пространства, то можно предположить, что и в других евроатлантических странах регулирующие органы, исследователи и организации гражданского общества, возможно, смогут использовать правила прозрачности DSA для повышения отзывчивости крупных платформ и технологических компаний, например США и Великобритании, к общественным ценностям тех обществ, интересам которых они призваны служить.

После брексита правительство **Великобритании** зеркально отражало европейское GDPR в своем национальном законодательстве 2018 г. — в **«Общем регламенте по защите данных Великобритании (UK GDPR»**, в который позже было внесено много изменений, когда в 2025 г. приняли Закон «**UK Data Act Use and Access» (DUAA)** с модификациями по защите и использованию данных и доступу к ним.

Важным средством регулирования цифрового пространства в Великобритании является и «Закон о безопасности в интернете» (**Online Safety Act**), принятый в 2023 г. и вступивший в силу марте 2025 г. Он юридически обязывает крупные платформы и поисковые системы предотвращать распространение вредоносного контента, защищать детей от материалов, не соответствующих их возрасту, и удалять незаконный контент. Также стоит отметить запрет к весне 2027 г. на **использование основных соцсетей: TikTok, Instagram, Facebook*** (*запрещенные на территории РФ) **детьми младше 16 лет**, причем с жестким контролем возраста, чтобы закон действительно работал.

В США за последние годы многочисленные члены Конгресса предложили законопроекты, в том числе «**Закон об ответственности и прозрачности платформ», «Закон о данных социальных сетей», «Закон о надзоре за цифровыми услугами», а также «Закон о безопасности детей в Интернете»,** которые усилили бы обязательства по обеспечению прозрачности в отношении практик модерации контента на платформах, онлайн-рекламы и мер по защите личных данных и детей. Но пока ни один из этих законов не был принят. Поэтому фактически частный сектор в отсутствие федерального законодательства в США по большинству вопросов, возникающих по регулированию информационного пространства, занимается **саморегулированием**, в которое Верховный суд США вмешивается только при острой необходимости.

При полном отсутствии единого федерального законодательства мы в США имеем дело с **«лоскутным одеялом регулирования»**. Так, например, в области ИИ одни штаты, например Колорадо, уже приняли комплексные законы об ИИ и защите потребителей, обязывающие разработчиков высокорисковых систем ИИ к предотвращению алгоритмической дискриминации. А в это время, другие штаты, как Калифорния пока только требуют от разработчиков публикации документации по обучающим данным моделей ИИ и нанесения водяных знаков, если медиаконтент сгенерирован с помощью ИИ. Но Калифорнийский закон о прозрачности ИИ **(California AI Transparency Act)** действует только для ИИ-фирм, число ежемесячных пользователей которых превышает 1 млн [16].

Некоторые другие штаты уже регулируют использование дипфейков и вводящих в заблуждение синтетических медиа (особенно в контексте политических выборов), а также имеются законы по применению ИИ в работе органов государства самого штата.

В мае 2026 г. Комитет по банковскому делу Сената США направил в Сенат федеральный законопроект «О прозрачности рынка цифровых активов» **(Digital Asset Market Clarity Act)**, сокращенно CLARITY Act, призванный положить конец многолетним конфликтам компетенций между регулирующими органами США и установить четкие правила по другой области цифровой экономики США, а именно относительно того, какие криптоактивы следует рассматривать как ценные бумаги, а какие — как сырьевые товары. При этом само законодательство не запрещает высокопоставленным чиновникам, в т. ч. президенту, вице-президенту и членам Конгресса, вести дела с криптовалютной индустрией во время своей госслужбы [8].

Рассматривая регулирование цифрового пространства в США, приходится констатировать, что в отличие от ЕС, там нет никакого всеобъемлющего федерального законодательства — ни по защите данных граждан, ни по регулированию электронной коммерции, социальных сетей или тем более сферы ИИ. Вместо этого существуют различные отраслевые федеральные рекомендации, а также разрозненный набор законов и законодательные механизмы по общей защите прав потребителей в отдельных штатах.

В США **нет и центрального органа надзора** за защитой данных или цифровых прав граждан, (такого как, например, отвечающие за соблюдение GDPR органы ЕС). На родине самых значимых интернет- и ИИ-гигантов контроль значительных технологических рисков в рамках своих обязанностей осуществляет **Федеральная торговая комиссия (FTC),** отвечающая за борьбу с недобросовестными или вводящими в заблуждение практиками в торговле и обеспечивающая соблюдение правил, запрещающих вводящие в заблуждение отзывы потребителей, в том числе сгенерированные ИИ. Кроме того, Федеральная **комиссия по связи (FCC)** регулирует цифровое пространство и массмедиа, в т. ч. на предмет отслеживания и предотвращения генерирования нежелательных автоматических звонков и подделывания голосов (deep fake). А **Комиссия по ценным бумагам и биржам (SEC)** обеспечивает соблюдение правил против мошенничества с использованием ИИ.

На современном этапе политика Белого дома в первую очередь сосредоточена на национальной безопасности, на продвижении технологических инноваций и достижении мировой гегемонии.

При этом именно сфера ИИ остается самой малорегулируемой на федеральном уровне в США. В марте 2026 г. Д. Трамп изложил **общие принципы в президентской стратегии по ИИ** «The White House's National Policy Framework for Artificial Intelligence» [19], содержащей законодательные рекомендации по формированию последовательного и единого на национальном уровне подхода к регулированию ИИ. Не имея прямой юридической силы, эта стратегия закладывает **основные принципы**, и особое внимание в ней уделяется вопросам защиты детей от незаконного контента, правам родителей для контроля использования ИИ детьми, расширению мощностей и инфраструктуры для ИИ, обучению и подготовке кадров для работы с ИИ, соблюдению прав интеллектуальной собственности, предотвращению цензуры, защите свободы слова, содействию инновациям и обеспечению доминирования США в сфере ИИ,

Уже в июне 2026 г. для дальнейшего регулирования этого важнейшего сегмента цифрового пространства президентом Д. Трампом был подписан **Executive Order (указ) 14409, по вопросам национальной безопасности в сфере ИИ**, в частности, добровольной оценке моделей с «открытыми границами», представляющих наибольшую угрозу, как говорилось ранее о модели Claude. Компаниям-разработчикам этот указ предлагает на добровольной основе предоставлять правительству доступ к новым «моделям, относящимся к сфере регулирования» за 30 дней до официального выпуска в целях оценки их безопасности. При этом подчеркивается, что «не предполагается обязательного предварительного согласования, выдачи разрешений или государственного лицензирования для разработки, публикации, выпуска и распространения новых моделей ИИ» [12].

В сентябре 2026 г. руководители фирм OpenAI, Anthropic и «X*» (запрещенной на территории РФ) в связи с угрозами, исходящими от моделей ИИ для будущего человечества сами предложили **замедлить темпы их разработки во избежание рисков** их выхода из-под контроля, пока не будут созданы правовые рамки для регулирования этих моделей ИИ. На это президент Трамп сначала ответил, что у него есть министерство юстиции и другие правоохранительные органы, которые возьмут ситуацию «под контроль», если надо, и что он будет поощрять развитие ИИ, потому что «кто победит по ИИ, победит во всём» [10].

После встречи с председателем КНР Си Цзиньпином в конце сентября 2026 г. он также отвергал необходимость согласования общих принципов регулирования ИИ с Китаем, который якобы года на полтора отстает от разработок США. Директор Anthropic тогда объявил об односторонней приостановке их дальнейших разработок моделей ИИ, проявляя еще раз чувство ответственности за безопасность моделей, в то время как президент Д. Трамп всему миру демонстрирует опаснейшее нежелание регулировать эту важнейшую для будущего мира сферу ИИ на общегосударственном и международном уровне.

Неслучайно, наверное, новый папа Римский Лев XIV. свою первую «Энциклику» посвятил именно исходящим от искусственного интеллекта угрозам для человечества. Настолько, получается, регулирование цифрового пространства на международном уровне отстает от необходимого уровня, что в послании особый акцент делается именно на этике использования ИИ, о которой нет смысла даже говорить, если «эта нравственность определяется немногими» [4, с. 107].

Заключение

Сравнительный анализ национального и наднационального правового регулирования цифрового пространства в Европе, Великобритании и США показал **большие различия** как в законодательстве этих стран, так и в правоприменительной практике. В то время, как **ЕС** применяет **самые строгие стандарты** в области конкурентной цифровой среды, защиты данных, свободы слова, прав личности, молодежи, пользователей и т. д, централизует полномочия по принятию решений в отношении глобального киберпространства в Брюсселе и строго формулирует санкции на законодательном уровне, чтобы затем, насколько это возможно, обеспечить их выполнение всеми активными в ЕС акторами, нынешняя администрация **США** во главу угла ставит не безопасность данных или моделей, а технологический прогресс, децентрализует принятие решений, перекладывая их с федерального на уровень отдельных штатов, и так старается добиться своей основной цели — **сохранения технологического превосходства** над самым крупным конкурентом в этой цифровой сфере — КНР, чьи высоко-инновационные услуги отчасти противоречат западной этике.

При рассмотрении реуляторских подходов США, КНР и ЕС, остается открытым вопросом, в какой степени европейское понимание права, с его ориентированностью на защиту данных и права человека, способно гарантировать национальным экономикам **ЕС цифровой суверенитет** в эпоху больших данных и ИИ, и не помешает ли гипертрофия защиты данных технологическому прогрессу в Европе.

Выявлены такие **недостатки европейского законодательства** по цифровой среде, как опасность превращения запретительных мер в инструмент цензуры, и в серьезную угрозу для альтернативных СМИ и свободы слова. И если, например, DMA по поводу «цифровых привратников» предусматривает разумное антимонопольное регулирование, то санкционные механизмы против нарушения прав пользователей на социальных платформах, пока только действуют для крупных онлайн-платформ, что является изъяном.

По вопросу **эффективности существующего регулирования** выявлено, что Евросоюз пока нерешительно применяет предусмотренные Законом о защите данных (DSA) и Законом об ИИ (AI Act) санкции в отношении американских гигантов в сфере ИИ и социальных сетей, и неслучайно, наверное, последняя попытка ЕС регулировать ИИ новыми «Правилами ответственности в сфере ИИ» (Liability Rules for Artificial Intelligence) в прошлом году потерпели крах за отсутствием консенсуса среди государств-членов и заинтересованных сторон. Так, именно **сфера искусственного интеллекта остается самой нерегулируемой**, — как в Европе, так и в США.

Остается надеяться, что вопросы регулирования и контроля над ИИ наконец станут приоритетными для всех мировых лидеров. И в заключение статьи хочется отметить, что как бы по-разному регуляторы стран мира подходили к законотворчеству, сегодня вопрос заключается не в том, кто «выиграет» гонку, а в том, как страны мира смогут быстро **учиться на опыте друг друга**, чтобы не отставать от систем, развивающихся с микросекундной скоростью.

Литература

1. Берман А. М. Правовое регулирование использования цифровых технологий в Германии и Евросоюзе // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2021. Т. 13, № 4. С. 127–137.
2. Гавриленко О. В. Цифровые технологии социального контроля: перспективы и социальные последствия их внедрения // Вестник Московского университета. Серия 18. Социология и политология. 2022. №1. с. 145-163 URL: https://vestnik.socio.msu.ru/jour/article/view/972 (дата обращения: 07.08.2026).
3. Карцхия А. А. Правовые аспекты регулирования информационной среды // 2025. №1. с. 19-31, URL: https://cyberleninka.ru/article/n/pravovye-aspekty-regulirovaniya-informatsionnoy-sredy (дата обращения: 08.08.2026)
4. Пиро И. Энциклика Льва XIV: ИИ на службе человечеству, а не горстке властителей. Ватикан, 26.05.2026 г., URL: https://www.vaticannews.va/ru/pope/news/2026-05/enciklika-lva-xiv-ii-na-sluzhbe-chelovechestvu-ne-vlasti-nemnogi.html (дата обращения: 07.08.2026).
5. Commission fines X €120 million under the Digital Services Act, 05.12.2025. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934 (дата обращения: 08.06.2026)
6. The EU Artificial Intelligence Act, 12.07.2024, URL: https://artificialintelligenceact.eu/the-act/ (дата обращения: 03.5.2026).
7. European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01), 23.01.2023, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2023_023_R_0001 (дата обращения: 09.08.2026).
8. H.R.3633 — 119th Congress (2025-2026): Digital Asset Market Clarity Act of 2025 URL: https://www.congress.gov/bill/119th-congress/house-bill/3633/text (дата обращения: 05.08.2026)
9. Kuehling J., Klar M., Sackmann F. Datenschutz. 6. Auflage, Heidelberg, C.F. Mueller, 2025, 460 S.
10. Mangan D. Trump says DOJ will rein in AI ‘if we have to’, 21.09.2026. URL: https://www.cnbc.com/2026/09/21/trump-ai-doj.html (дата обращения 22.09.2026)
11. Philippot F. L' Arcom va désigner ses "signaleurs de confiance" comme SOS Racisme, 10.11.2025. URL: https://www.dailymotion.com/video/x9u1vq0 (дата обращения: 30.04.2026)
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. Promoting Advanced Artificial Intelligence Innovation and Security. Executive Order 14409 of June 2, 2026. URL: https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/ (дата обращения 30.09.2026).
14. 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.
15. 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
16. SB 942 California AI Transparency Act, 20.09.2024. URL: https://www.leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942 (дата обращения 07.07.2026).
17. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, URL: https://dsgvo-gesetz.de/art-5-dsgvo/ (дата обращения 07.06.2026).
18. Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2065 (дата обращения 07.06.2026).
19. The White House’s National Policy Framework for Artificial Intelligence, 03.03.2026, URL: https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf (дата обращения 27.09.2026).

THE DIGITAL SPACE: EXPERIENCES WITH ITS LEGAL REGULATION IN EURO-ATLANTIC COUNTRIES

Tatunts, Svetlana A.

Doctor of sociology, Ph.D. in historical sciences, professor
Moscow State University named after M. V. Lomonosov
Faculty of World Politics
Full Professor
Moscow, Russian Federation
S.Tatunts@fmp.msu.ru

Abstract

The regulation of the digital space knows no borders and is a priority, given the rapid pace of technological development. In this article, the author analyzes the experience of EU, UK and the U.S. in this field, including issues related to the regulation of AI and the associated threats. European legislation and enforcement practices are examined in detail. At the theoretical level, the regulatory models of the EU, the US, and China – which differ fundamentally in their objectives and ethical principles – are compared. The conclusion is drawn that the European regulatory system (GDPR, DSA, DMA, EU AI Act, including their British counterparts) is highly effective, whereas regional legislation at the state level in the U.S. is fragmented, with a complete absence of federal legislation governing the digital space. Using a paradigmatic methodological approach and specific examples from the digital economies of the countries under study, the article calls for a prompt revision of the world wide regulation of the digital space.

Keywords

regulation; digital space; data protection; GDPR; DSA; DMA; AI

References

1. Berman A.M. Pravovoe regulirovanie ispol'zovanija cifrovyh tehnologij v Germanii i Evrosojuze // Territorija novyh vozmozhnostej. Vestnik Vladivostokskogo gosudarstvennogo universiteta jekonomiki i servisa. 2021. T. 13, # 4. C. 127–137.
2. Gavrilenko O.V. Cifrovye tehnologii social'nogo kontrolja: perspektivy i social'nye posledstvija ih vnedrenija // Vestnik Moskovskogo universiteta. Serija 18. Sociologija i politologija. 2022. #1. pp. 145-163 Available at: https://vestnik.socio.msu.ru/jour/article/view/972 (accessed: 07.08.2026).
3. Karchija A.A. Pravovye aspekty regulirovanija informacionnoj sredy // 2025. #1. pp. 19-31, URL: https://cyberleninka.ru/article/n/pravovye-aspekty-regulirovaniya-informatsionnoy-sredy (accessed: 08.08.2026).
4. Piro I. Jenciklika L'va XIV: AI na sluzhbe chelovechestvu, a ne gorstke vlastitelej. Vatikan, 26.05.2026 g. Available at: https://www.vaticannews.va/ru/pope/news/2026-05/enciklika-lva-xiv-ii-na-sluzhbe-chelovechestvu-ne-vlasti-nemnogi.html (accessed: 07.08.2026).
5. Commission fines X €120 million under the Digital Services Act, 05.12.2025, URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934 (accessed: 08.06.2026).
6. The EU Artificial Intelligence Act, 12.07.2024, URL: https://artificialintelligenceact.eu/the-act/ (accessed: 03.5.2026).
7. European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01), 23.01.2023, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2023_023_R_0001 (accessed: 09.08.2026).
8. H.R.3633 — 119th Congress (2025-2026): Digital Asset Market Clarity Act of 2025. URL: https://www.congress.gov/bill/119th-congress/house-bill/3633/text (accessed: 05.08.2026).
9. Kuehling J., Klar M., Sackmann F. Datenschutz. 6. Auflage, Heidelberg, C.F. Mueller, 2025, 460 S.
10. Mangan D. Trump says DOJ will rein in AI 'if we have to', 21.09.2026 URL: https://www.cnbc.com/2026/09/21/trump-ai-doj.html (accessed 22.09.2026).
11. Philippot F. L' Arcom va désigner ses "signaleurs de confiance" comme SOS Racisme, 10.11.2025. URL: https://www.dailymotion.com/video/x9u1vq0 (accessed: 30.04.2026).
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. Promoting Advanced Artificial Intelligence Innovation and Security. Executive Order 14409 of June 2, 2026 URL: https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/ (accessed: 30.09.2026).
14. 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.
15. 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.
16. SB 942 California AI Transparency Act, 20.09.2024 URL: https://www.leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942 (accessed: 07.07.2026).
17. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, URL: https://dsgvo-gesetz.de/art-5-dsgvo/ (accessed: 07.06.2026).
18. Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste). URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2065 (accessed: 07.06.2026).
19. The White House's National Policy Framework for Artificial Intelligence, 03.03.2026, URL: https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf (accessed: 27.09.2026).