

УДК 342.5

**ПОЛИТИКО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТ-КОММУНИКАЦИИ:  
ОПЫТ ЗАРУБЕЖНЫХ СТРАН****А. В. КРЕМНЕВ***(Представлено: канд. ист. наук, доц. А. Л. РАДЮК)*

*Данная статья посвящена анализу политико-правового регулирования интернет-коммуникации на примере конкретных стратегий зарубежных стран. Автор статьи рассматривает различные способы регулирования оборота информации в сети Интернет. На основе проведенного исследования автор делает вывод о связи между политико-экономическими характеристиками государств и их подходов к регулированию интернет-коммуникации.*

Стремительная цифровизация и формирование информационного общества послужили причинами резкой популяризации и внедрения коммуникационных технологий в различные сферы жизнедеятельности человека. Особую роль в данном процессе играет интернет-коммуникация, которая больше не является простым средством взаимодействия с друзьями, коллегами и родственниками, а становится полноценным инструментом воздействия на важнейшие процессы, протекающие в современном обществе. Такой массовый феномен не мог остаться без внимания со стороны государственных институтов, он послужил для них своего рода толчком к изучению возможностей и практике регулирования интернет-коммуникаций с целью преодоления возможных негативных последствий. Существование полноценной сети Интернет длится уже более четверти века, однако на международном уровне до сих пор не было выработано конкретных нормативных правовых актов, в общем порядке регламентирующих отношения в данной сфере. Несмотря на определённое количество различных международных деклараций, конвенций и договоров, государствам в данном вопросе предоставляется вся широта полномочий, что подразумевает под собой детерминированность регулирования интернет-коммуникаций различными особенностями политической и правовой системы конкретного государства. В связи с этим опыт нормативно-правового регулирования Интернет-коммуникаций в зарубежных странах можно рассмотреть только на конкретных примерах.

В соответствии с различными исследованиями уровня свободы в сети Интернет на территории конкретного государства, Соединенные Штаты Америки характеризуются наиболее свободным Интернет-пространством [1]. Государственные органы США, несмотря на определённые риски прибегают к стратегии наименьшего вмешательства в процесс регулирования сети Интернет. Подобная стратегия обусловлена, во-первых, тем, что США являются исторической родиной Интернета, а также тем, что многие IT-компании (Google, Facebook, Twitter и др.), занимающие лидирующее место в сфере Интернет-коммуникаций, базируются непосредственно в США. Во-вторых, первая поправка к конституции США напрямую запрещает государственным органам принимать законы или совершать иные действия, ограничивающие свободу слова граждан и свободу прессы [2]. В-третьих, невероятные успехи в экономике и роль мирового гегемона в политике позволяет США диктовать свои условия иностранным государствам и добиваться от них выполнения своих требований, в том числе касающихся защиты интересов американских IT-компаний, что говорит об определённом сотрудничестве между государственной властью и крупными транснациональными корпорациями.

Основная задача законодателя в сфере регулирования Интернет-коммуникации в США сводится к деятельности по защите информации частного характера и интеллектуальной собственности, а также к обеспечению условий честной конкуренции торговли в сети Интернет и в реальном мире [3, с. 4]. В связи с тем, что государственные органы не обладают полномочиями по фильтрации информации в сети Интернет, этим фактически занимаются крупные IT-компании, владеющие интернет-платформами. Основным актом, регулирующим оборот информации в различных онлайн-платформах, выступают пользовательские соглашения и правила сообщества. Так, в правилах сообщества популярной социальной сети Twitter установлен запрет на публикацию контента, который связан с угрозой насилием, призывами к террористическим актам, сексуальной эксплуатацией малолетних, оскорблениями, преследованиями или дискриминацией по различным признакам и т.д. [4]. Примерно таким же образом сформулированные запреты, содержащиеся в пользовательских соглашениях социальных сетей Facebook, Instagram, YouTube и др. Подобная свобода IT-компаний по фильтрации контента на своих площадках по своим же правилам не является фактом, подтверждающим отсутствие цензуры интернет-коммуникации в США, напротив возникает серьезный риск цензуры со стороны IT-компаний. Фактически, в США крупные транснациональные корпорации, владеющие популярными интернет-площадками, обладают огромной властью формировать отношение к публичным мероприятиям, подвергать цензуре или скрывать неудобную для определённых кругов информацию, тем самым влияя на политические и экономические процессы как внутри США, так и за рубежом.

Однако несмотря на первую поправку к Конституции, в США всё-таки имеется ряд законов, тем или иным образом регулирующих сферу Интернет-коммуникации. Так, например, Закон «О защите детей в Интернете» от 21 декабря 2000 года позволяет фильтровать Интернет-контент в учебных заведениях, который вреден для несовершеннолетних [5]. Также к косвенным методам фильтрации информации в сети Интернет относятся федеральный закон «О надзоре за внешней разведкой» от 25 октября 1978 года и федеральный закон «О сплочении и укреплении Америки путём обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» от 11 сентября 2001 года. Данные нормативные правовые акты наделяют правоохранительные органы США весьма широкими полномочиями по мониторингу интернет-трафика. Так, например, в соответствии с данными законами, правоохранительные органы на законной основе имеют право потребовать от телекоммуникационных компаний предоставить данные о местонахождении, электронной корреспонденции и интернет-трафике пользователей интернет-ресурса [3, с. 4]. Однако в целом, система регулирования Интернет-коммуникации в США остается крайне либеральной.

В европейских странах, в частности в странах Западной Европы, применяется в целом схожая с США стратегия регулирования интернет-коммуникации, но с определёнными оговорками и национальными особенностями. Так, в Федеративной Республике Германия был принят Закон «О мерах в отношении социальных сетей» от 30 июня 2017 года, вступивший в законную силу с 1 января 2018 года. Суть данного нормативного правового акта заключается в том, что он обязывает крупные социальные сети и интернет-площадки, насчитывающие два и более миллиона пользователей, оперативно удалять незаконный контент, нарушающий уголовное законодательство. При этом перечень незаконного контента является действительно объёмным: от оскорбления представителя государственной власти до разжигания ненависти и вражды между различными социальными группами. Санкцией за несоблюдение данного требования выступает штраф в размере до 50 миллионов евро. При этом в 2021 году было внесено дополнение к данному нормативному правовому акту. Закон, помимо фильтрации контента, в случае поступления более 100 жалоб на незаконный контент, обязывает социальные сети и иные интернет-платформы публиковать отчеты на немецком языке, в которых должна содержаться развернутая информация о том, как интернет-ресурсы справляются с этими жалобами [6]. Фактически, данный нормативный правовой акт является попыткой законодателя ФРГ переложить функцию цензора на владельцев интернет-ресурсов, и как показывает практика, достаточно успешно. Несмотря на выступления правозащитных организаций, интернет-ресурсы, опасаясь серьезных штрафов, уже в первые дни действия данного закона, начали активно удалять спорный контент. Таким образом, формально в ФРГ цензуры информации в сети Интернет нет, т.к. государство де-юре не вмешивается в данную сферу.

Во Французской Республике с 15 февраля 2011 года действует закон «О безопасности Интернета», который устанавливает определённые меры регулирования, в том числе осуществление обязательной фильтрации контента в сети Интернет для пресечения распространений детской порнографией на основании составляемых Министерством внутренних дел Франции совместно с различными общественными организациями и активистами т. н. «чёрных списков». Помимо порнографического контента, фильтрации подвергается контент, связанный с распространением антисемитских и расистских взглядов. При этом любой ресурс, заподозренный в распространении опасного контента, может быть незамедлительно подвергнут блокировке по представлению МВД Франции, судебное решение в такой ситуации не требуется. Для борьбы с террористическими группами, использующим Интернет-коммуникации, в МВД Франции создано специальное подразделение – «кибер-патруль». Задача данного подразделения состоит в выявлении и сборе доказательств в отношении лиц, участвующих в подстрекательстве к терроризму или в осуществлении террористических актов. Для реализации поставленных задач, сотрудники данного подразделения под вымышленными именами принимают участие в интернет-форумах, состоят в сообществах в социальных сетях и контактируют с лицами, подозреваемыми в терроризме [7]. Также между Правительством Франции и Великобританией в 2018 году был согласован план совместных действий по повышению эффективности выявления и удаления контента, характеризующегося как террористический, экстремистский или разжигающий ненависть и вражду. Суть совместных действий состоит в требовании от крупных IT-компаний автоматизировать процесс выявления незаконного контента и ускорить его блокировку или удаление, а также предоставлять доступ к зашифрованному трафику правоохранительным органам [8].

Великобритания, в отличие от континентальной Европы, характеризуется более проработанной законодательной базой, регулирующей общественные отношения, связанные с передачей информации при помощи Интернет-коммуникации. Первый нормативный правовой акт в данной сфере был принят в 2003 году. Это был закон «О коммуникациях» от 25 июля 2003 года, который контролирует создание независимого регулятора коммуникационного пространства. В 2004 году Парламент Великобритании принял закон «О чрезвычайных ситуациях», помимо всего прочего в законе закреплено право Правительства Великобритании определять режим работы средств цифровой передачи данных, в т.ч. право на полное отключение данных средств и прекращение Интернет-коммуникации на территории государства [9, с. 3]. Далее, 8 апреля 2010 года был принят закон «О цифровой экономике», регулирующий вопросы перехода страны на цифровое телевидение, вопросы радиовещания, особенности издания видеоигр и защиту авторского права в сети Интернет. Однако особый интерес с точки зрения регулирования Интернет-коммуникации

вызывает специфическая санкция за нарушения правил пользования средствами Интернет-коммуникации или за грубые и систематические нарушения авторского права в сети Интернет, которая выражается в лишении возможности пользоваться средствами Интернет-коммуникации конкретного в индивидуальном порядке по требованию уполномоченного Министерства. При этом, если Интернет-провайдер по каким-либо причинам не выполнит поручение государственного органа, то ему будет грозить штраф в размере 250 тысяч фунтов стерлингов [10]. В 2014 году был принят закон «Об истребовании персональных данных», который обязал интернет-площадки и провайдеров хранить все данные пользователей на протяжении года и в случае необходимости предоставлять к ним доступ правоохранительным органам Великобритании [11].

В целом можно сказать, что страны Западной Европы скорее склонны к либеральному подходу в отношении нормативного регулирования Интернет-коммуникаций. Законодатели этих государств стараются найти определённый баланс между конституционным правом на доступ к информации и поддержанием общественной безопасности [3, с. 4]. Однако Великобритания в данном вопросе выделяется попыткой подробного регулирования данной сферы, что объясняется тем, что ментально и культурно Великобритания стоит особняком от государств континентальной Европы.

Менее либеральным подходом к Интернет-коммуникации характеризуется Российская Федерация, в которой выработана весьма массивная нормативно-правовая база, регулирующая оборот информации в сети Интернет. Базовыми законодательными актами в данной области являются Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» и Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которые устанавливают основы данных правоотношений. Однако действительно серьезное влияние на Интернет-коммуникацию в России оказал Федеральный закон от 28 июля 2012 г. № ФЗ-139, благодаря которому появился «Единый реестр запрещенных сайтов». Также этот закон внёс в другие законы ряд положений, суть которых заключалась в фильтрации интернет-ресурсов по системе «черного списка» и оперативной блокировке запрещенных интернет-ресурсов [12, с. 226]. Данный закон стал платформой для дальнейшего ужесточения законодательства в сфере Интернет-коммуникации, что вызывало шквал критики в адрес данного закона со стороны активистов и правозащитных организаций. Однако несмотря на это, уже в конце 2013 года был принят Федеральный закон от 28 декабря 2013 г. № 398-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”», суть которого состоит в наделении Роскомнадзора полномочием по предписанию Генеральной Прокуратуры Российской Федерации осуществлять немедленную блокировку интернет-ресурсов без решения суда, распространяющих призывы к массовым беспорядкам или информацию, носящую экстремистский характер [13, ст. 1]. Таким образом произошло установление контроля не только над Интернет-коммуникацией в общем виде, но и над политической Интернет-коммуникацией. Особый общественный резонанс в Российской Федерации вызвали федеральные законы № 374-ФЗ и № 375-ФЗ, принятые в 2016 году, которые повысили срок хранения операторами мобильной связи и Интернет-ресурсами информации о фактах приема, передачи и содержимого голосовой информации и сообщений от полугода до трех лет, а позволил следователям получать информацию из электронной переписки пользователей социальных сетей и мессенджеров [12, с. 227]. А уже 25 ноября 2017 году Федеральным законом №327-ФЗ были внесены изменения в Закон Российской Федерации «О средствах массовой информации», которые обязывают все СМИ (в т.ч. различные Интернет-ресурсы), получающие финансирование из-за рубежа, пройти регистрацию как иностранные СМИ, выполняющие роль иностранного агента. Помимо этого, данный Федеральный закон предусматривает внесение изменений, позволяющих осуществлять быструю внесудебную блокировку сайтов организаций, признанных «нежелательными» на территории Российской Федерации [15]. На этом ужесточение законодательства в данной сфере не прекратилось, буквально каждый последующий год принимались новые законы и вносились изменения в действующие, с целью ужесточения оборота информации при помощи Интернет-коммуникации.

Одним из наиболее «свежих» Федеральных законов Российской Федерации, регулирующих сферу Интернет-коммуникации, является Федеральный закон от 30.12.2020 г. № 530-ФЗ, которым были внесены изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации». Суть изменений заключается в борьбе с распространением фейков в социальных сетях. Закон распространяется на владельцев соцсетей более чем с 500 тыс. пользователей за сутки, он обязывает их создать в России представительство публичной сети, вести реестр заявлений пользователей и предоставлять его контролирующим органам по первому требованию. Также владельцы социальных сетей обязаны по требованию пользователей удалять информацию, за распространение которой предусмотрена уголовная или административная ответственность [16].

В целом, резюмируя все сказанное о правовом регулировании Интернет-коммуникации в Российской Федерации, можно сделать вывод о том, что в данном государстве взят курс на подчинение интернет-коммуникации государственным интересам и максимально возможное правовое регулирование данной сферы. При этом Российская Федерация на сегодняшний день не является государством, полностью контролирующим Интернет-коммуникации на своей территории, а скорее иллюстрацией планомерного перехода от либерального отношения к государственному контролю сети Интернет.

Хрестоматийным примером жёсткого государственного регулирования Интернет-коммуникации традиционно является Китайская Народная Республика, в связи с установленным в ней особым политическим режимом. Особенностью регулирования Интернет-коммуникации в КНР является наличие сложной системы регулирования политического контента, состоящая из трёх элементов: системы фильтрации трафика, системы блокировки поиска нежелательной информации, ручной системы фильтрации контента, публикуемого в социальных сетях и других интернет-площадках [17, с. 6]. В первых двух случаях подразумевается работы системы «Золотой щит», которая создана с целью осуществления прямой государственной цензуры всего интернет-пространства КНР. Иностраные сайты, в содержание которых входит наличие политически некорректной информации с точки зрения властей КНР подвергаются блокировке. Интернет-ресурсы, базирующиеся на территории КНР, не имеют право ссылаться и публиковать новости, взятые из зарубежных новостных сайтов или СМИ, без специального одобрения уполномоченных органов. Помимо этого, данная система не просто не дает доступ к черному списку сайтов, но и скрывает определённые поисковые запросы, по ключевым словам, осуществляя таким образом фильтрацию информации, которую может получить рядовой гражданин КНР при вводе какого-либо поискового запроса [17, с. 4]. Из-за такой сложной обстановки, ряд популярных интернет-площадок заблокированы на территории КНР.

Также, помимо автоматической системы, в Китае роль фильтра информации выполняют десятки тысяч цензоров, однако они принимаются за дело только в случае, когда негативный информационный повод грозит перерасти в волну недовольства и вылиться в массовые протестные акции или политические движения. В такой ситуации цензоры предпринимают различные меры по разрушению коммуникативных связей между пользователями, а также всячески препятствуют обсуждению темы. При этом важно отметить, что при отсутствии критической ситуации, которая могла бы перерасти в крупные скандалы и массовые волнения, критические высказывания в адрес государственного аппарата или действий отдельных чиновников не возбраняются [17, с. 7].

Жёсткому контролю подвергаются не только интернет-ресурсы, но и пользователи. Так, Закон «О кибербезопасности» от 7 ноября 2016 года существенно ограничивает анонимность за счет введения требования об обязательной верификации для доступа к сети. Так, если пользователь не предоставляет свои реальные индикаторные данные, то Интернет-провайдер не имеет права предоставить ему доступ в Интернет. Помимо этого, власти КНР имеют право замораживать активы иностранных физических лиц в случае, если они подозреваются в осуществлении действий, наносящих вред информационной национальной инфраструктуре [18].

Суммируя факты, можно сделать вывод о том, что КНР является примером осуществления жесткой государственной цензуры Интернет-коммуникации на своей территории, однако различные ограничения, налагаемые на данную сферу, касаются именно общественно-политического пространства. Китаем выбран путь на создание собственной информационной инфраструктуры, независимой от остального мира.

Таким образом, на основе анализа зарубежной практики правового регулирования Интернет-коммуникации можно сделать вывод о том, что наиболее либеральный подход в данной области характерен для США и государств Западной Европы. Российская Федерация представляет собой переходный вариант между либеральным регулированием и жестким государственным контролем. Китай в свою очередь является беспрецедентным примером подчинением Интернет-коммуникации государственному аппарату. Также наблюдается определённая связь между политико-экономическими характеристиками государства и стратегией регулирования Интернет-коммуникации. Так, менее либеральный подход характерен для государств, политический режим которых можно охарактеризовать как авторитарный или имеющий черты авторитарного. При этом государства, выбравшие стратегию, направленную на жесткое регулирование интернет-коммуникации, обладают большим населением и обширными территориями, а также экономически и культурно могут обеспечить свою независимую национальную информационную инфраструктуру или же оказать воздействие на транснациональные корпорации, являющиеся владельцами популярных интернет-ресурсов. При этом, несмотря на выбранную стратегию, все государства уделяют большое внимание защите авторского права и борьбе с контентом, оказывающий деструктивное воздействие как на отдельно взятого индивида, так и на социум в целом.

## ЛИТЕРАТУРА

1. Freedom on the NET 2021 [Electronic resource] : Freedom House. – Mode of access: <https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech>. – Date of access: 16.05.2022.
2. Конституция США 1787 г. [Электронный ресурс] // Электронная библиотека Исторического факультета МГУ им. М. В. Ломоносова. – Режим доступа: <http://www.hist.msu.ru/ER/Etext/cnstUS.htm>. – Дата доступа: 16.05.2022.
3. Ваховский, А. М. Политико-правовые вопросы регулирования Интернета: мировой опыт и Российская практика / А. М. Ваховский // Известия Тульского государственного университета. – 2016. – № 2. – С. 3–11.
4. Правила Twitter [Электронный ресурс] // Справочный центр Twitter. – Режим доступа: <https://help.twitter.com/ru/rules-and-policies/twitter-rules>. – Дата доступа: 16.05.2022.

5. Children's Online Privacy Protection Rule [Electronic resource] : Federal Trade Commission. – Mode of access: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>. – Date of access: 16.05.2022.
6. Act to Improve Enforcement of the Law in Social Networks [Electronic resource] : Federal Ministry of Justice. – Mode of access: [https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG\\_engl.pdf?\\_\\_blob=publicationFile&v=2](https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2). – Date of access: 16.05.2022.
7. Правовое регулирование сегментов Интернета [Электронный ресурс] // Центр политической информации. – Режим доступа: [http://polit-info.ru/images/data/gallery/0\\_9764\\_regulirovanie\\_interneta.pdf](http://polit-info.ru/images/data/gallery/0_9764_regulirovanie_interneta.pdf). – Дата доступа: 16.05.2022.
8. United Kingdom – France summit communique 18 January 2018 [Electronic resource] : Statewatch. – Mode of access: <https://www.statewatch.org/media/documents/news/2018/jan/uk-fr-summit-communique.pdf>. – Date of access: 16.05.2022.
9. Шишигин, И. И. Кибербезопасность как основное направление развития правовых норм в условиях цифровой экономики: международные тренды / И. И. Шишигин, И. В. Николаева // Научно-методический электронный журнал Концепт. – 2019. – № 12. – С. 194–200.
10. Закон Великобритании «О цифровой экономике» (Digital Economy Act 2010) [Электронный ресурс] // Lex Digital Blog. – Режим доступа: <http://lexdigital.ru/2012/03/>. – Дата доступа: 16.05.2022.
11. Data Retention and Investigatory Powers Act 2014 [Electronic resource] : legislation.gov.uk. – Mode of access: <https://www.legislation.gov.uk/ukpga/2014/27/contents>. – Date of access: 16.05.2022.
12. Пивоваров, В. А. Политико-правовое регулирование интернет-пространства в России / В. А. Пивоваров // Известия Саратовского Университета. Новая серия. – 2018. – № 2 (18). – С. 225–231.
13. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] : Федер. закон, 28 дек. 2013 г., № 398-ФЗ : в ред. Федер. закона от 28.12.2013 г. // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2022.
14. Роскомнадзор прекращает вести реестр блогеров [Электронный ресурс] // Роскомнадзор. – Режим доступа: [https://rkn.gov.ru/news/rsoc/news48342.htm?utm\\_source=ru.wikipedia.org&utm\\_medium=referral&utm\\_campaign=ru.wikipedia.org&utm\\_referrer=ru.wikipedia.org](https://rkn.gov.ru/news/rsoc/news48342.htm?utm_source=ru.wikipedia.org&utm_medium=referral&utm_campaign=ru.wikipedia.org&utm_referrer=ru.wikipedia.org). – Дата доступа: 16.05.2022.
15. О внесении изменений в статьи 10-4 и 15-3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 6 Закона Российской Федерации «О средствах массовой информации» [Электронный ресурс] : Федер. закон, 25 ноя. 2017 г., № 327-ФЗ : в ред. Федер. закона от 25.11.2017 г. // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2022.
16. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] : Федер. закон, 30 дек. 2020 г., № 530-ФЗ : в ред. Федер. закона от 30.12.2020 г. // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2022.
17. Линь, Д. Основы правового регулирования и административного контроля Интернета в Китае / Д. Линь // Административное право и практика администрирования. – 2020. – № 2. – С. 1–9.
18. Горян, Э. В. Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы / Э. В. Горян // Административное и муниципальное право. – 2020. – № 3. – С. 1–9.