УДК 340.1:004
ББК 67.408.135

СОВРЕМЕННЫЕ ПРОБЛЕМЫ И ВЫЗОВЫ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ФЕЙКОВИЗАЦИИ ИНТЕРНЕТА

О. А. Голубцова, С. И. Меженская
Луганский государственный университет им. В. Даля (Луганск, Россия)

Авторами анализируется роль государства в разработке антифейковых мер. Раскрыты последствия и угрозы от распространения фейков в сети Интернет. Отмечено, что в мире существует два подхода к сфере ответственности за распространение фейковой информации. Анализируются функции государства в решении проблемы распространения фейков, в частности фальшивых новостей. Исследуется процесс государственного регулирования относительно противодействия фейковизации интернета в российском законодательстве. Отмечено, что фейковые новости представляют собой огромную проблему современного мира, правовое регулирование в данной сфере имеет ряд пробелов, что создает сложности выявления фальшивой информации, а также назначения наказания за ее распространение.

В ходе исследования была выдвинута идея внедрения в качестве эффективного подхода в борьбе с фейковизацией интернета международных концепций, принципов и идей: разработка и стандартизация соответствующей нормативно-правовой базы на базе успешного опыта других стран.

Авторы обосновали направления совершенствования отечественной правовой системы по противодействию фейковизации интернета.

Ключевые слова: фейковые новости, фейковизация интернета, государственное регулирование, противодействие фальшивым новостям

MODERN PROBLEMS AND CHALLENGES OF STATE REGULATION OF INTERNET FAKING

O. A. Golubtsova, S. I. Mezhenskaya
Lugansk State University named after Vladimir Dahl (Lugansk, Russia)

In the article, the authors analyzed the role of the state in the development of anti-fake measures. The consequences and threats from the spread of fakes on the Internet are revealed. It is noted that there are two approaches in the world to the sphere of responsibility for the dissemination of fake information. The functions of the state in solving the problem of the spread of fakes, in particular fake news, are analyzed. The article examines the process of state regulation regarding countering the fake Internet in Russian legislation. It is noted that fake news is a huge problem in the modern world, legal regulation in this area has a number of gaps, which makes it difficult to identify fake information, as well as to impose penalties for its dissemination.

In the course of the study, the idea was put forward as an effective approach to combating Internet faking, the introduction of international concepts, principles and ideas: the development and standardization of an appropriate regulatory framework based on the successful experience of other countries.

The authors have substantiated the directions of improving the domestic legal system to counteract the fake Internet.

Keywords: fake news, fake Internet, government regulation, countering fake news

Doi: https://doi.org/10.14258/ralj(2025)1.6

Совершенствование технологий сети Интернет привело к тому, что социальные веб-сервисы и медиаресурсы становятся все более масштабными и глубоко интегрированными в повседневную жизнь. Благодаря легкому доступу к ним потенциальные пользователи получают ин-

формацию и обмениваются ею, а также могут высказывать и распространять различные сообщения. Из-за открытости социальных сетей, большого количества пользователей и, как следствие, различных источников информации происходит фейковизация интернета (формируются так называемые фейковые новости, или фейки). Фейки в сети Интернет распространяют специально обученные специалисты, чтобы ввести рядовых читателей в заблуждение. Такая информация может нанести серьезный моральный вред как непосредственно читателям, так и обществу в целом, а также вызвать значительные политические и экономические потери. Причина в том, что у рядовых пользователей нет времени и навыков проверять достоверность прочитанной информации. Поэтому перед соответствующими государственными службами встает неотложная задача выявлять такие фейковые новости в социальных сетях, как-то их обозначать или даже удалять, т. е. гарантировать слабо ориентированным читателям получение достоверной информации.

Как свидетельствует исторический анализ развития человечества, технологии распространения фейковой информации не являются абсолютно новыми, поскольку они в том или ином виде всегда сопровождали конфликтные ситуации. Однако именно в последние годы они начали играть большое значение в международных и внутринациональных конфликтах, экономических, политических, культурных и других процессах.

В частности, рассмотрению данной проблемы посвящены работы Н. А. Марковой, А. С. Кургановой, Д. Бебич, М. Воларевич, С. В. Полищук, М. О. Зыряновой и др.

В этих работах сделан вывод о том, что эффективное противодействие данной угрозе может быть реализовано только посредством комплексного подхода, включающего в себя в том числе разработку соответствующего правового инструментария.

Цель статьи — исследование опыта правового противодействия фейковизации интернета.

Юридический аспект исследования данной проблемы должен включать сравнительно-правовой анализ существующих подходов к определению и нормативному закреплению категории «фейк», «фейковая» информация», «фейк/фейковые новости». Совершенно очевидно, что история содержит еще много подобных примеров. В то же время если явление распространения лжи насчитывает уже много веков, то понятие «фейк/фейковые новости» (fake news) достаточно новое. Как отмечается в словаре Мериам-Вебстер (Merriam-Webster), понятие fake news в англоязычном информационном пространстве появилось в конце XIX в., распространилось использование прилагательного fake/fake news — «поддельные / поддельные новости» вместо false/false news — «ложные / ложные новости». Между этими словами существует разница, которая позволяет установить между ними определенные родовидовые отношения: false означает прежде всего «ложный» (not true), «некорректный» (incorrect), в то же время fake есть не просто «ложный» (not true), но «имитирующий «(imitation), поддельный» (counterfeit), т. е. характеризует явления и предметы, копирующие, имитирующие те, которые реально существуют. Именно такое содержание понятия определяет одну из основных черт фейковых новостей — имитационность. Понятие претерпело несколько существенных трансформаций, в результате чего образовалось широкое поле его значений.

В мире существует два подхода к сфере ответственности за распространение фейковой информации. Первый (европейский) предусматривает гражданско-правовое урегулирование ответственности за диффамацию в медиа и ответственность за распространение фейков. Второй — уголовное преследование за распространение такой деструктивной информации как частных лиц, так и СМИ. Только скоординированные усилия органов власти путем налаживания эффективного межгосударственного взаимодействия и совершенствования нормативно-правовой базы с использованием современных технологий защиты информации позволят повысить уровень информационной безопасности государства и отдельных граждан [1 с. 63].

Пассивная роль государства в разработке антифейковых мер не позволяет создать соответствующее правовое поле, способное обеспечить информационные права граждан в условиях масштабных дезинформационных кампаний. Кроме того, передача основных рычагов влияния другим (негосударственным) структурам может привести к дублированию ими функций государства. К примеру, частные технологические компании (Big Tech), действуя против распространения фальшивых новостей, регулируют контент и информационную повестку дня для пользователей, порой перебирая на себя функции государственных регуляторов [2, с. 284].

Основными функциями государства в решении проблемы распространения фейков, в частности фальшивых новостей, являются прежде всего такие:

— четкая публичная позиция государства по противодействию распространению фейков;
— формирование правового поля (дефиниции, стандарты, создание государственных регуляторов / изменение их полномочий, формулирование требований к провайдерам и регистраторам доменных имен и т. п.) и введение действенных санкций за нарушение его положений;
— организация и финансирование исследований, посвященных проблемам воздействия, распространения и противодействия фейкам в Интернете;
— аккумулирование и обеспечение обмена информацией, касающейся дезинформационных кампаний (в частности, обмен информацией для частных компаний, медиа, а также обмен информацией между структурами безопасности, законодательным органом и частными структурами);
— распространение медиаграмотности как основы формирования национальной устойчивости к воздействиям фейков;
— организация обучения государственных служащих, дипломатов способам распознавания возможностей и каналов влияния фейковой информации, способам противодействия ее распространению;
— создание условий для развития медиасреды;
— поддержка усилий частных структур, медиа, общественных организаций для противодействия распространению фальшивых новостей;
— оценивание мероприятий по противодействию распространению фальшивых новостей (дезинформации) и распространение этих данных на широкую общественность.

Одним из приоритетных направлений совершенствования отечественной правовой системы по противодействию фейковизации интернета является внедрение международных концепций, принципов и идей. В качестве эффективного подхода в борьбе с фейковизацией интернета видится выработка и стандартизация соответствующей нормативно-правовой базы.

В российском законодательстве сделаны первые шаги относительно правового противодействия фейковизации интернета. Федеральный закон от 18 марта 2019 г. № 31-ФЗ „О внесении изменений в статью 15-3 Федерального закона „Об информации, информационных технологиях и о защите информации”» дополняет перечень видов информации, распространяемой с нарушением закона, и закрепляет на законодательном уровне категорию «фейковая информация», под которой следует понимать «недостоверную общественно значимую информацию, распространяемую под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращению функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи».

Стоит отметить поправки, внесенные в УК РФ в 2020 г. в ст. 207.1, 207.2, криминализующие, по сути, аналогичные деяния, что и п. 10.1, 10.2 ст. 13.15 КоАП РФ, а именно «публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и (или) о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств» (ст. 207.1), а также «публичное распространение под видом достоверных сообщений заведомо ложной общественно значимой информации, повлекшее по неосторожности причинение вреда здоровью человека (ч. 1 ст. 207.2), по неосторожности смерть человека или иные тяжкие последствия (ч. 2 ст. 207.2)».

Разграничение административной ответственности, предусмотренной ст. 13.15 КоАП РФ, и уголовной ответственности, предусмотренной ст. 207.1, 207.2 УК РФ, проводится исходя из критерия субъектного состава, поскольку административная ответственность за правонарушения, предусмотренная п. 10.1 и 10.2 ст. 13.15 КоАП РФ, установлена для юридических лиц, а граждане, должностные лица и руководители юридических лиц могут быть привлечены к уголовной ответственности, предусмотренной ст. 207.1 и 207.2 УК РФ.

На международном уровне первыми документами в сфере борьбы с фейками в интернете стали Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 г., и дополнительный протокол к Конвенции, направленный на борьбу с распространением через компьютерные сети информации расистского и ксенофобского характера от 28 января 2003 г. В США в 1986 г. был принят первый нормативно-правовой документ противодействия киберпреступлениям — Закон о мошенничестве с использованием компьютеров — Computer Fraud and Abuse Act (CFAA), основный федеральный закон, криминализирующий несанкционированный доступ к компьютерным системам и сетям [3]. Помимо указанного закона, США имеют развитую правовую базу для борьбы с киберпреступностью, которая включает ряд законов и нормативных актов:

— Electronic Communications Privacy Act (ECPA), регулирует перехват и мониторинг электронных коммуникаций;
— USA PATRIOT Act, расширяет возможности правоохранительных органов в борьбе с терроризмом и киберпреступностью;
— Cybersecurity Information Sharing Act (CISA), способствует обмену информацией о киберугрозах между правительством и частным сектором, и др.

Противодействие фейковизации интернета в США является комплексным и многоуровневым процессом, который включает законодательные, технологические и организационные мероприятия. Различные федеральные агентства играют ключевую роль в противодействии киберпреступности:

— Федеральное бюро расследований (FBI) — основной орган, занимающийся расследованием киберпреступлений, включая хакерские атаки, финансовые мошенничества и кражи данных;
— Агентство по кибербезопасности и безопасности инфраструктуры (CISA) — подразделение внутренней безопасности, отвечающее за обеспечение безопасности критической инфраструктуры;
— Национальное агентство безопасности (АНБ) — отвечает за мониторинг и защиту национальных сетей от киберугроз.

США активно внедряют передовые технологии для обнаружения и противодействия фейковизации интернета.

Важным аспектом противодействия киберпреступности является повышение осведомленности и обучения. Противодействие фейковизации интернета в США является многогранной и интегрированной деятельностью, которая включает правовые, технологические и образовательные мероприятия. Благодаря активному сотрудничеству между государственными органами, частным сектором и международными партнерами США создают эффективную систему защиты от киберугроз.

В Великобритании существует свой нормативно-правовой документ — Акт о компьютерных злоупотреблениях, принятый в 1990 г., предусматривающий наказание за совершение преступления в компьютерном пространстве: штраф или лишение свободы на срок от 6 месяцев до 5 лет. В Нидерландах и Германии противодействие киберпреступности ведется путем введения новых статей в действующий уголовный кодекс [4, с. 1375].

В Европейском Союзе, участницами которого являются 27 стран, нормативно-правовыми актами, принятыми для противодействия противоправным посягательствам на электронные информационные ресурсы, является Директива ЕС по противодействию кибератакам на информационные системы, 2013 г.; Директива Еврокомиссии по борьбе с мошенничеством и другими финансовыми преступлениями в сети Интернет. В ЕС значительное внимание уделяется проблематике раннего выявления и оперативного реагирования на фейковизацию интернета.

Создание специальных подразделений полиции в сфере противодействия киберпреступности, и в частности фейковизации интернета, практикуется во многих странах мира: Австралии, Бельгии, Великобритании, Германии, Дании, Индии, Канаде, Малайзии, Нидерландах, Норвегии, Польше, США, Швейцарии, Швеции, Эстонии и др.

Франция является государством, которое одним из первых в Европе приняло меры к усилению роли государства в регулировании киберпространства [5, с. 98]. В сфере активной борьбы с киберпреступностью 14 февраля 2008 г. была принята французская стратегия по борьбе с киберпреступностью, целью которой является сотрудничество между частным бизнесом (поставщиками информационно-телекоммуникационных услуг) и правоохранительными органами по обмену информацией и вопросам объединения усилий в борьбе с киберпреступностью.

Парламент Сингапура одобрил закон, направленный на борьбу с фейковыми новостями. Законом предусмотрена уголовная ответственность за умышленное распространение фейковой информации в виде лишения свободы сроком на 10 лет и наложение штрафа в размере до 1 млн сингапурских долларов. Также в соответствии с законом государственные органы могут потребовать внесения виновным лицом поправок или удаления контента. Кроме того, органам государственной власти предоставляется право блокировать сайты, распространяющие недостоверную общественно значимую информацию.

В последние десятилетия угроза фейковизации интернета превратилась в острую проблему, требующую координации действий на международном уровне. Операторы сети Интернет обязаны обеспечить понятный и доступный для пользователей способ сообщения о наличии негативного контента [6, с. 171].

Европейские институты в указанных документах артикулируют следующие основные меры противодействия распространению дезинформации (фальшивых новостей):

— внесение изменений в национальные законы с целью учесть возможные угрозы, возникающие в результате кампаний по дезинформации, в частности по адаптации избирательных правил к проведению онлайн-кампаний;
— усиление защиты персональных данных (с целью их неиспользования, например, для распространения таргетированных фальшивых новостей), в частности через создание законодательных положений об использовании данных;
— контроль политической рекламы (размещение информации о заказчиках, указание на собственных сайтах партий такой же информации, как и для политической рекламы в интернете);
— создание сети фактчекеров, которую поддерживают национальные правительства, и академических исследователей дезинформации в различных социальных сетях и цифровых медиа;
— создание онлайн-платформы по защите от дезинформации (Secureonline Platform on Disinformation);
— быстрый обмен информацией в режиме реального времени. Реализацией того шага является создание в марте 2019 г. системы быстрого оповещения (Rapid Alert System, RAS), состоящей из контактных пунктов на уровне государств —членов (National Contact Points) для быстрого обмена информацией, в частности об использовании дезинформации, в режиме реального времени;
— обмен опытом по борьбе с нарушениями, в частности с распространением дезинформации. С этой целью создана Европейская сеть электорального сотрудничества.

Фейковые новости представляют собой настоящую проблему современного мира, с каждым днем она становится более масштабной, их все труднее обнаруживать даже квалифицированным специалистам. Главная проблема, с которой сталкиваются законодатели, — баланс между свободами человека и сохранением общественных интересов. Даже в тех странах, где конституция запрещает принимать закон, ограничивающий свободу слова, сегодня предпринимаются попытки урегулировать фейковые новости, что воспринимается неоднозначно.

Сегодня очень сложно противодействовать фейковизации интернета, но в ведущих государствах мира осуществляются дальнейшие поиски нормативных механизмов противодействия фейкам, диффамации в социальных медиа. Что касается борьбы с распространением дезинформации, необходимо четко различать разные типы феномена фейковых новостей: политическую пропаганду, журналистские ошибки, сатиру, вымышленные новости в целях экономической выгоды. Однако универсальных рецептов борьбы с фейками до сих пор не существует. Общепризнанным остается ориентация на то, что эталоном защиты от деструктивной пропаганды и манипуляции сознанием человека является прежде всего прочность демократических традиций каждого общества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Голубцова О. А. Международный опыт правового противодействия фейковизации информационного пространства // Российско-азиатский правовой журнал. 2024. № 1. С. 62–66.

2. Дерюгин А. А., Луценко В. В. Противодействие распространению «фейковой» информации в вопросах обеспечения безопасности: функция государства в современных условиях // Ученые записки

Крымского федерального университета им. В.И. Вернадского. Юридические науки. 2022. Т. 8, № 3. С. 281–286.

3. Аверьянова А.А. Административно-правовые средства противодействия «фейкам» в РФ // Дневник науки. 2022. № 10.

4. Манойло А.В., Теличко В.И., Попадюк А.Э. Особенности организации противодействия фейковым новостям // Вопросы политологии. 2021. Т. 11, № 5. С. 1374–1381.

5. Захарова М.В. Фейковая информация и имидж политика: эффекты, модели противодействия (опыт Франции) // Век информации. 2022. № 2–2. С. 98–99.

6. Поздняков Е.И. Гражданское общество как субъект противодействия фейк-ньюс в системе информационной безопасности России и Китая // Гражданин. Выборы. Власть. 2022. № 4. С. 170–178.