

# ОСОБЕННОСТИ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ ИНДИВИДУАЛЬНЫХ СУБЪЕКТОВ ПРАВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

**Минаева Анастасия Игоревна**

Аспирант, Московского государственного  
юридического университета им. О.Е. Кутафина  
(МГЮА)

law.minaeva@gmail.com

## THE FEATURES OF LEGAL RESPONSIBILITY OF INDIVIDUAL SUBJECTS OF LAW IN THE CONDITIONS OF DIGITALIZATION

**A. Minaeva**

*Summary.* The subject of this article is the influence of the digitalization process on the views of legal science on such a legal category as legal liability. The author explores classical approaches to the concept and signs of legal responsibility of individual subjects of Russian law, as well as their changes in the conditions of digitalization. The author considers the question of the special digital responsibility of individual subjects of law. Also, the author, through the study of fundamentally new offenses committed on the Internet, comes to the conclusion that it is necessary to amend the current criminal legislation, as well as the legislation on administrative offenses. In addition, the author explores the issue of a high degree of depersonalization of offenders in the context of the use of digital technologies, as well as the emergence of fundamentally new measures of legal responsibility.

*Keywords:* individual subjects of law, legal responsibility, cyberbullying, cybersquatting.

*Аннотация.* Предмет рассмотрения настоящей статьи — влияние процесса цифровизации на сложившиеся в правовой науке взгляды на такую правовую категорию, как юридическая ответственность. Автор исследует классические подходы к понятию и признакам юридической ответственности индивидуальных субъектов российского права, а также их изменение в условиях цифровизации. Автор рассматривает постановку вопроса об особой цифровой ответственности индивидуальных субъектов права. Также автор посредством исследования принципиально новых правонарушений, совершаемых в сети «Интернет» приходит к выводу о необходимости внесения изменений в действующее уголовное законодательство, а также в законодательстве об административных правонарушениях. Кроме того, автор исследует вопрос о высокой степени деперсонализации правонарушителей в условиях использования цифровых технологий, а также о появлении принципиально новых мер юридической ответственности.

*Ключевые слова:* индивидуальные субъекты права, юридическая ответственность, кибербуллинг, киберсквоттинг.

**В** современном мире активно развиваются и распространяются цифровые технологии, которые стали причиной пристального внимания современной правовой науки к роли цифровых технологий, перспективам их развития, особенностям их проникновения во всю структуру права. В условиях фактически тотальной цифровизации подверглись трансформации и система права, и сама юридическая наука.

Категория юридической ответственности в правовой науке занимает особое место и подвергается пристальному вниманию ученых-правоведов. Так, под юридической ответственностью понимают «особую разновидность социальной ответственности, направленную на выполнение юридической обязанности и воплощающуюся в обеспечительных мерах убеждения, поощрения и наказания» [1, с. 10].

Как правило, среди признаков юридической ответственности выделяется то, что она основана на государственном принуждении; наступает после совершения правонарушения; выражается в наступлении негативных последствий для нарушителя, которые являются для него обязательными, и которых не было до совершения им правонарушения; лишения могут иметь личный и имущественный характер; исполняется в процессуальной форме.

Традиционной является классификация юридической ответственности в зависимости от характера (вида) правонарушения. В связи с этим большинство юристов выделяют уголовную, административную, дисциплинарную, гражданско-правовую и материальную, конституционную. В рамках каждого из указанных видов юридической ответственности необходимо ис-

следовать особенности, порождаемые цифровым пространством.

Уголовная (уголовно-правовая) ответственность представляет собой наиболее суровый вид ответственности репрессивно-штрафного характера. Она устанавливается уголовным законом за совершение какого-либо общественно опасного деяния, причинившего или способного причинить вред наиболее значительным общественным отношениям.

В настоящее время действующее уголовное законодательство предусматривает юридическую ответственность за преступления, совершаемые в том числе с использованием цифровых технологий (в частности, ст. 110, ст. 110.1, ст. 110.2, ст. 151.2, ст. 171.2, ст. 185.3, ст. 228.1, ст. 238.1 Уголовного кодекса Российской Федерации).

Учеными-правоведами предлагаются новые термины, обозначающие различные злоупотребления правами граждан посредством использования цифровых технологий, в частности:

- ◆ киберсквоттинг (регистрация доменных имен с использованием обозначений, которые, по предположениям регистрирующих их лиц, в будущем могут понадобиться кому-либо настолько, что будут выкуплены у них по цене, в несколько раз превышающей расходы на регистрацию доменного имени);
- ◆ обратный киберсквоттинг (отбор права на широко известное доменное имя посредством регистрации соответствующего ему товарного знака);
- ◆ организация DDoS-атак (атака на вычислительную систему с целью довести её до отказа, то есть, создание таких условий, при которых пользователи системы не могут получить доступ к ресурсам системы) и участие в них, распространение незапрашиваемой информации, троллинг (проявление различных форм агрессивного и оскорбительного поведения, нарушающих этику сетевого взаимодействия) [2, с. 137].

В науке отмечается, что создание нормативных правовых актов, регулирующих вопросы цифровизации различных сфер жизни общества, должно сопровождаться оценкой возможных рисков с целью быстрого создания и изменения уголовно-правовых норм, охраняющих соответствующие общественные отношения и права личности [3, с. 146].

Второй вид юридической ответственности, традиционно выделяемый в правовой науке — административная ответственность. Административная ответственность наступает за совершение правонарушений

в сфере государственного и общественного порядка, осуществления прав и свобод граждан, а также установленного порядка управления.

В настоящее время действующее законодательство об административных правонарушениях предусматривает юридическую ответственность индивидуальных субъектов права за правонарушения в цифровой среде (в частности, ч. 3 ст. 6.17, ч. 2 ст. 6.21, ч. 3 ст. 6.33, ч. 1 ст. 14.1.1 Кодекса об административных правонарушениях Российской Федерации).

Посредством анализа положений уголовного законодательства и законодательства об административных правонарушениях можно сделать вывод, что в настоящее время активно разрабатываются составы преступлений, связанных с действиями индивидуальных субъектов права в цифровой среде, что, безусловно, является большим шагом на пути к обеспечению правовой определенности общественных отношений в этой сфере и к обеспечению эффективной защиты прав человека. Однако, к сожалению, правовые нормы не успевают за теми отношениями, которые уже фактически складываются в цифровом пространстве.

Так, например, в настоящее время большое внимание ученых посвящено проблеме «кибербуллинга», который обычно принимает форму запугивания и угроз через сотовые телефоны или компьютер с доступом к Интернету посредством социальных сетей, форумов, онлайн-чатов, электронной почты и так далее. В настоящее время существует множество определений кибербуллинга.

Понятие кибербуллинга дается в Письме Минобрнауки России от 14.05.2018 № 08–1184: преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Так, заслуживает внимания следующее определение кибербуллинга — это «умышленное виновно совершенное действие или совокупность действий, направленных на психологическое подавление жертвы, причинение ей нравственных страданий, осуществляемых посредством электронных средств связи» [4, с. 92]. При этом предлагается также выделять определенные виды кибербуллинга:

- ◆ клевета (вид буллинга, при котором используется распространение заведомо ложной информации);
- ◆ харрасмент (неоднократная отправка оскорбительных текстовых или иных файлов, адресованных, как правило, конкретному человеку);
- ◆ киберпреследование (выслеживание жертвы с помощью интернет-ресурсов для организации

вымогательства, нападения, шантажа, избиения и т.д.);

- ◆ хеппислепинг (снятие на видео реальных сцен насилия, избиения, убийств с последующим его размещением в сети «Интернет»);
- ◆ самозванство (вид кибербуллинга, при котором агрессор представляет себя как жертву, используя ее пароль для доступа к ее аккаунту в социальных сетях либо создав страницу от имени жертвы и осуществляя негативную коммуникацию с другими пользователями);
- ◆ перепалки (обмен короткими оскорбительными репликами между двумя или более людьми, происходящий чаще всего в публичных местах Сети (комментарии в блогах, социальных сетях));
- ◆ доксинг (публичное раскрытие личных и конфиденциальных данных через Интернет).

В целом наиболее распространенными примерами кибербуллинга являются: получение унижительных и угрожающих сообщений; распространение компрометирующих фотографий, обидных постов в целях унижения потенциальной жертвы; создание поддельных профилей человека; взлом аккаунта в социальной сети в целях оказания психологического давления на жертву; распространение интимной или дискредитирующей информации о человеке.

Относительно ответственности киберагрессора в России необходимо отметить, что в действующем законодательстве не предусмотрена ответственность за кибербуллинг как самостоятельный состав преступления.

Необходимость правового регулирования противодействия кибербуллингу является очевидной и насущной задачей, в настоящее время необходимо закрепить понятие кибербуллинга, определить его виды и формы, установить меру ответственности.

Кроме того, особенности уголовной ответственности в цифровом пространстве связаны с возможностью для злоумышленников «скрываться» в пространстве так называемого «Даркнета» («Darknet»),

Даже при надежной идентификации субъекта правонарушения, наличия в законодательстве состава киберпреступления правонарушитель может «скрываться» в этом абсолютно нерегулируемом «теневом» мире в цифровом пространстве, однако это не означает, что указанные выше правонарушения не должны подвергаться правовому регулированию.

Следующие виды юридической ответственности — дисциплинарная и материальная ответственность, ко-

торая возникает вследствие совершения дисциплинарных проступков, то есть за нарушения трудовой, учебной, воинской, служебной дисциплины. Дисциплинарная ответственность наступает за проступки, которые совершаются виновными лицами в процессе осуществления ими трудовой деятельности, исполнения своих служебных обязанностей.

В условиях развития цифровых технологий, встал, например, вопрос о проблеме использования сети «Интернет» на рабочем месте и возможности привлечения работника к ответственности за нарушение трудового режима, в связи с чем в правовой науке обосновывается введение в действующее законодательство запрета на использование социальных сетей в рабочее время [5, с. 160].

Кроме того, при дистанционной работе (осуществлении трудовой деятельности посредством использования цифровых технологий) могут возникать нарушения трудовой дисциплины, связанные не с умыслом работника, а с особенностями работы технического оборудования (например, работник в 9 утра должен явиться на совещание, однако он не может «подключиться» к нему в «Zoom» из-за отсутствия интернет-подключения или нестабильной работы необходимого технического оборудования), что необходимо рассматривать при решении вопроса о привлечении работника к дисциплинарной ответственности.

И, наконец, гражданско-правовая ответственность предусмотрена за нарушение договорных обязательств или за причинение внедоговорного имущественного ущерба, то есть за совершение гражданско-правового деликта. Ее сущность состоит в принуждении лица нести отрицательные имущественные последствия.

Мерами гражданско-правовой ответственности, как и в других видах юридической ответственности, являются лишь те, которые связаны с дополнительными обременениями для правонарушителя, то есть выступают для него в виде определенного наказания за совершенное правонарушение. Эти обременения могут быть в виде возложения на правонарушителя дополнительной гражданско-правовой обязанности или лишения принадлежащего ему субъективного гражданского права.

Большая часть правонарушений в сети «Интернет» связана с нарушением прав на результаты интеллектуальной деятельности: в основном это распространение произведений без разрешения (лицензии) правообладателей.

Примером незаконного использования объектов интеллектуальной собственности при размещении

информации на интернет-сайте могут служить получившие широкое распространение в сети Интернет так называемые музыкальные архивы (MP3-архивы), электронные библиотеки, галереи фотографий, видеоархивы. Как правило, размещение информации в данных архивах происходит без ведома автора и правообладателя, без выплаты им вознаграждений за использование их произведений, авторские договоры не заключаются. Размещение (воспроизведение) произведения на интернет-сайте возможно только на основании договора с правообладателем/автором либо его соответствующего разрешения. Если у владельцев интернет-сайта нет такого разрешения (договора), значит, нарушаются авторские права, защищаемые законом (объем нарушения определяется в каждом конкретном случае). Лица, права и интересы которых нарушены в результате ненадлежащей рекламы, вправе обратиться в установленном порядке в суд с исками, в том числе с исками о возмещении убытков, включая упущенную выгоду, компенсации морального вреда.

Следовательно, по таким правонарушениям виновным лицом считается тот пользователь, который первым в нарушении авторских прав распространил то или иное произведение без согласия автора в сети «Интернет».

Относительно признаков юридической ответственности индивидуальных субъектов права в цифровом пространстве можно отметить следующее.

Обычно среди признаков юридической ответственности выделяется то, что меры юридической ответственности закрепляются действующим законодательством. Однако в контексте цифровых правоотношений необходимо исходить из того, что меры юридической ответственности предусмотрены не только (а зачастую и не столько) законодательством, но и самими цифровыми технологиями (например, такая мера как блокировка пользователя, отключение от сети «Интернет»).

Кроме того, в рамках классического подхода правоведы исходят из того, что юридическая ответственность всегда связана с государственным принуждением, которое строго регламентируется законом и не выходит за его рамки. Причем это не принуждение вообще, а «мера» принуждения, четко очерченный его объем. Однако и здесь необходимо исходить из того, что меры, которые применяются, например, администрацией социальных сетей или оператором поисковой системы («Яндекс», «Google») с очевидностью не имеют характера государственного принуждения, так как осуществляются ими по собственному усмотрению. Иногда блокировка доступа может быть «случайной», например,

из-за влияния вредоносного программного обеспечения («вируса»).

В-третьих, по общему правилу юридическая ответственность применяется только специально уполномоченными органами, однако меры ответственности за те или иные действия в сети «Интернет» связаны преимущественно не с решениями уполномоченных органов, а опять-таки с действиями самих цифровых систем.

В-четвертых, по общему правилу необходимым условием наступления юридической ответственности является наличие вины, которое выражается в неблагоприятных последствиях для правонарушителя, в форме умысла или неосторожности. На наличие такого умысла может указывать осведомленность лица о технических возможностях программ (в том числе в силу его компьютерной грамотности). В некоторых случаях (например, при прохождении процедуры регистрации в социальных сетях) подписание пользователем «Пользовательского соглашения», в котором закреплен запрет на размещение контента определенного вида, может свидетельствовать об осведомленности лица о том, что его действия носят незаконный характер и могут повлечь за собой юридическую ответственность.

Следовательно, при определении умысла правонарушителя необходима специальная техническая экспертиза с целью выяснения, не была ли произведена атака вредоносной программой, предусматривающей возможность дистанционного запуска программного обеспечения и как следствие осуществление определенных действий вообще без ведома владельца технического устройства. Для установления умысла правонарушителя необходимо в каждом конкретном случае устанавливать наличие либо отсутствие у лица особых технических знаний, проводить оценку действий, совершаемых лицом в процессе размещения файлов, определять, имело ли место их последующее удаление [6, с. 83].

Кроме того, юридическая ответственность предполагает лишение правонарушителя некоторых социальных благ (свободы, права занимать определенные должности, имущества и др.). В рамках юридической ответственности за правонарушения, совершенные в цифровом пространстве, возможно лишение правонарушителя такого блага как доступа к объектам цифрового пространства (например, при блокировке доступа пользователя к сети «Интернет», блокировка аккаунтов).

Необходимо исходить из того, что основание для привлечения к юридической ответственности — правонарушение при наличии полного его состава.

Можно выделить два основания юридической ответственности: юридическое (предписания нормы права, предусматривающей тот или иной вид юридической ответственности) и фактическое (совершение правонарушения). Юридическая ответственность за действия в цифровом пространстве предполагают в определенной степени совпадение: и мера ответственности, и совершение правонарушения могут находиться в единой плоскости — плоскости цифровых технологий.

В цифровом пространстве мы видим в рамках применения некоторых мер ответственности отсутствие правоотношения между индивидуальным субъектом ответственности и государством, так как действия осуществляются исключительно посредством самих цифровых технологий, посредством заложенных в сетевую систему определенных алгоритмов.

Анализ пользовательских соглашений, разработанных «Яндексом», «Google», «Instagram», «ВКонтакте» и некоторых других цифровых сервисов, с правилами которых пользователь «соглашается» при получении доступа к ним и начале их использования, позволяет выявить следующие меры ответственности, которые этими соглашениями предусмотрены:

- ◆ частичное или полное удаление контента (размещенные пользователем разного рода информация и материалы);
- ◆ временная или постоянная блокировка доступа к сервисам;
- ◆ блокировка или удаление учетной записи по собственному усмотрению оператора;
- ◆ полный отказ пользователю в использовании сервисов оператора;
- ◆ ограничение доступа к учетной записи, блокировка учетной записи пользователя, а также запрет доступ с использованием какой-либо учетной записи к определенным сервисам оператора;
- ◆ удаление почтового ящика сервисе, если пользователь не пользовался им более 24 месяцев;
- ◆ отказ пользователю в размещении и/или распространении им контента или удаление любого контента, который доступен посредством цифровых сервисов.

В контексте использования цифровых технологий особое значение, как представляется, имеет позитивная ответственность — это мера требовательности к себе и другим, понимание интересов общества и государства. В отличие от негативной, позитивная ответственность не временная и не принудительная, а постоянная и добровольная ответственность личности за своё поведение в настоящем и в будущем за надлежащее исполнение своих юридических обязанностей. Это своего рода мера требовательности к себе. Необходимо отметить, что в цифровом пространстве на сегодняшний день индивидуальные субъекты права действуют наиболее свободно, поскольку цифровые отношения строятся на основе того, насколько развиты сами цифровые технологии, какие меры реакции на нарушения тех или иных правил предусмотрены самой цифровой инфраструктурой. Следовательно, позитивная ответственность как добровольная ответственность за свое поведение проявляется наиболее активно. Однако ее, безусловно, недостаточно для построения стабильного правопорядка.

Юридическая ответственность в условиях развития цифровых технологий предопределяет постановку вопроса об особой «цифровой ответственности» индивидуального субъекта права, которая обладает следующими особенностями: в рамках применения некоторых мер отсутствует правоотношение между индивидуальным субъектом ответственности и государством; применяются специфические для цифровой среды меры юридической ответственности (частичное или полное удаление контента, временная или постоянная блокировка доступа к объектам цифровой инфраструктуры); существование особого порядка идентификации субъекта юридической ответственности, определяемого цифровыми технологиями и, как следствие, высокая степень деперсонификации субъекта правонарушения; опосредованность юридической ответственности в цифровой среде не столько реализацией санкций правовых норм, сколько действием самих цифровых технологий, алгоритмами искусственного интеллекта, особенностями программного обеспечения, действием различных агрегаторов, операторов, владельцев объектов цифровой инфраструктуры; отсутствие, как правило, четкой формализованной процессуальной формы привлечения к юридической ответственности.

#### ЛИТЕРАТУРА

1. Малько А.В., Маркунин Р.С. Правовая система общества и юридическая ответственность // Юридическая наука и правоохранительная практика. Тюмень, 2020. № 2. С. 6–13.
2. Середа В.Н., Середа М.Ю. Защита прав и свобод человека и гражданина в сети Интернет. Воронеж, 2013. 252 с.
3. Грачева Ю.В., Коробеев А.И., Маликов С.В., Чучаев А.И. Цифровизация и ее уголовно-правовые риски // Журнал «Правосудие» 2019. Т. 1 № 2. С. 133–155.

4. Бочкарева Е.В., Стренин Д.А. Теоретико-правовые аспекты кибербуллинга // Всероссийский криминологический журнал. 2021. т. 15. № 1. С. 91–97.
5. У.И. Николаенко Соблюдение трудовой дисциплины (использование Интернета и социальных сетей, телефонных разговоров на рабочих местах) // Символ науки. № 5. 2016. С. 158–160.
6. Кириллова Н.М. Размещение материалов и предметов порнографического содержания в сети «Интернет»: особенности уголовной ответственности// Вестник Московского университета. Серия 11: Право № 6. 2019. С. 75–85.

© Минаева Анастасия Игоревна ( law.minaeva@gmail.com ).

Журнал «Современная наука: актуальные проблемы теории и практики»



Московский государственный юридический университет имени О.Е. Кутафина