ст. 128 ГК. К примеру, энергия, газ, нефть и нефтепродукты, вода являются объектами гражданских прав в силу главы 30 ГК, они отнесены к оборотоспособному имуществу – товарам, а электромагнитный сигнал – нет».

Обращаясь к международным нормам, Международная конвенция об охране прав исполнителей, производителей фонограмм и вещательных организаций от 26 октября 1961 г., именуемая Римской, признает объектом смежных прав сигнал. Однако нормы данной конвенции устанавливают объекты правом охраны интеллектуальной собственности – «публикацию», «воспроизведение», «передачу в эфир», «ретрансляцию», а не объекты гражданских прав, в том числе не объекты интеллектуальной собственности (И. Н. Ковалевич).

Проанализировав данные точки зрения, стоит отметить, что наиболее близкой кажется идея охраны контента, нежели электромагнитного сигнала. Важной составляющей изображения является его наполненность, поэтому стоило бы охранять прежде всего информацию и контент, а не сам сигнал и технические способы его передачи. В связи с этим передачу организации эфирного или кабельного вещания можно определить следующим образом: «передача, создаваемая самой организацией эфирного или кабельного вещания либо по ее заказу другой организацией за счет ее средств, как совокупность звуков и (или) изображений или их отображений для приема публикой».

Решение вопроса о соотношении терминов «передача организации эфирного или кабельного вещания», «передача в эфир», «передача по кабелю» возможно путем внесения изменений в Закон. Здесь стоит обратиться к Закону Федеративной Республики Германия от 9 сентября 1965 г. «Об авторском праве и смежных правах» по состоянию на 23 июня 2021 г., где схожий термин в разделе 5, содержащем нормы об охраны прав телерадиокомпаний, «передача в эфир» заменен на «право транслировать». В связи с этим считаем обоснованным заменить термин «передача в эфир» термином «трансляция в эфир», соответственно термин «передача по кабелю» – термином «трансляция по кабелю».

Внесение данных изменений и дополнений в ст. 4 Закона «Об авторском праве и смежных правах», по нашему мнению, будет способствовать совершенствованию правоприменительной практики и устранению пробелов и терминологических противоречий.

Кузьменкова К. Д.

ВНЕДРЕНИЕ КОНЦЕПТА СУВЕРЕННОЙ ЦИФРОВОЙ ЛИЧНОСТИ В МЕХАНИЗМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Кузьменкова Кристина Дмитриевна, студентка 3 курса Белорусского государственного университета, г. Минск, Беларусь, law.kuzmenkoKD@bsu.by

Научный руководитель: канд. юрид. наук, доцент Ядревский О. О.

Цифровая личность определяется как набор проверенных цифровых атрибутов и учетных данных для цифрового мира, аналогичных идентичности человека для реального мира в идеальном понимании, а также

онлайновая или сетевая личность (идентификация), принятая или заявленная в киберпространстве отдельным лицом, организацией или электронным устройством. Выделяют три модели цифровой личности (в том числе идентификации): централизованная (основанная на аккаунте личность), с участием третьей стороны и децентрализованная или суверенная.

Централизованная модель предполагает совокупность идентификаторов и учетных данных (паспорта, водительские удостоверения и т. д.), которые выдаются государством лицу, что размещаются и находятся в зависимости от сторонних платформ. Данная модель также носит название личности (идентификации), основанной на аккаунте сервис-провайдера в сети Интернет, что связано с ее содержанием: личности не существует без аккаунта в какой-либо централизованной системе, доступ к которому есть у сервис-провайдера. Отличие модели «объединенной личности» или «пользовательско-центричной идентификации» от централизованной состоит в том, что в отношениях между компанией с данными и пользователем посередине появляется новый провайдер. Когда пользователь заходит на какую-либо стороннюю платформу, он может запросить доступ и предоставить данные с промежуточного провайдера. Наибольшее применение данная модель нашла в потребительской сети Интернет. Недостатками данных моделей является отсутствие реального владения своими персональными данными, постоянные утечки данных, торговля ими, реклама, основанная на наблюдении.

На смену первых двух концептов цифровой личности в 2015 г. появилась основанная на технологии блокчейна децентрализованная личность или децентрализованная модель идентификации (математическая). Согласно этой модели, (полная) идентичность сущности на самом деле распределяется в различных частичных идентичностях, действительных в пределах разных доменов разных предприятий (организаций). Основное отличие данной модели в том, что она больше не полагается на централизованные либо на объединенные провайдеры учетных данных, а также то, что она больше не основана на аккаунтах. Содержание данного концепта в следующем: он работает как идентификация в реальном мире, т. е. модель основана на прямом взаимодействии субъекта и другого участника стороны в форме однорангового узла. Никто не может контролировать или владеть этими отношениями. Позднее данную модель личности назвали моделью или концептом суверенной цифровой личности (англ. – self sovereign identity, далее – SSI).

SSI определяется как: а) набор принципов о том, как идентичность и управление персональными данными должны работать через цифровые сети; б) набор технологий, которые опираются на основные концепции в управлении идентификацией, распределенное вычисление, блокчейн или технологию распределенной книги и криптографию; в) протокол идентификации. Хотя в настоящее время не существует глобального стандарта для реализации SSI, наиболее распространенные компоненты технологии SSI предлагаются Консорциумом World Wide Web3 и Фондом

децентрализованной идентификации. В общих чертах структура SSI состоит: 1) учетные или цифровые данные (англ. verifiable credentials); 2) «Треугольник доверия» – эмитент, владелец и верификатор; 3) цифровые кошельки; 4) цифровые агенты; 5) децентрализованные идентификаторы (англ. decentralized identifiers); 6) блокчейн и другие регистраторы учетных данных.

Несмотря на инновационность и сложность разработки технологии, на данный момент уже сформировалась определенная практика применения концепта SSI. В качестве положительной практики можно выделить следующие законодательные акты, регулирующие использование концепта SSI: Панканадская система доверия, Гражданский кодекс Калифорнии (для выпуска и хранения медицинских персональных данных), Европейская структура суверенной идентификации (eSSIF), внедрение Hyperledger Indy Правительством Британской Колумбии, Онтарио и Канады, разработка цифровой версии карты резидента Министерством внутренней безопасности США. Невзирая на признание на законодательном уровне SSI, по-прежнему существует юридическая и нормативная неопределенность, однако вопрос внедрения нового концепта цифровой личности постепенно становится приоритетным для государственных регуляторов и крупного бизнеса. SSI является эффективным не только с точки зрения нового уровня защиты персональных данных, но и с позиции сокращения государственной бюрократии, формирования более эффективной системы здравоохранения, выявления академического мошенничества, улучшения банковского обслуживания, помощи в создании более эффективной системы распределения гуманитарной помощи и помощи компаниям в предотвращении утечки персональных данных и штрафов согласно законодательству о защите персональных данных.

Приведенная в пример и проанализированная практика внедрения SSI в рамках защиты персональных данных зарубежных стран дает возможность спрогнозировать перспективы развития и сформировать перечень предложений, уместных в контексте правового механизма защиты персональных данных в Республике Беларусь.

Так, на наш взгляд, целесообразными будут следующие предложения:

- в действующих законодательных актах либо разработанном комплексном акте необходимо закрепить понятия электронной идентификации, эмитента, верификатора, учетных данных, сервис-провайдера (агента), цифровых кошельков, блокчейна, децентрализованных идентификаторов;
- обеспечить и легализировать применение SSI физическими лицами и юридическими частными и государственными лицами;
- описать механизмы управления элементами SSI;

Считаем необходимым проведение более детальных исследований и анализа данной сферы.