

ции формальных требований к участию общественности в нормотворческой деятельности (на ее первых стадиях) для обеспечения большей доступности права и повышения гражданской активности белорусов.

Библиографические ссылки

1. Дробязко, С. Г. Общая теория права : учеб. пособие для вузов / С. Г. Дробязко, В. С. Козлов. – 3-е изд., испр. и доп. – Минск : Амалфея, 2009. – 484 с.

НЕКОТОРЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ ПРАВА НА ИДЕНТИЧНОСТЬ В ЦИФРОВОЙ СРЕДЕ

Маркевич Дарья Сергеевна,

аспирант кафедры теории и истории государства и права
Белорусского государственного университета (г. Минск)
dasha.markevich@gmail.com

Важной особенностью цифровой среды является то, что для нее в меньшей степени справедливы правила и законы реального мира. Это проявляется в том, что, с одной стороны, индивид получает неограниченную свободу в выборе инструментов и моделей поведения, а, с другой стороны, существует меньше гарантий реализации и защиты его субъективных прав. При этом конвергенция реального и цифрового мира требует разработки и внесения системы норм и предписаний, в том числе гарантируемых силой государственного принуждения. В связи с чем, категориально-понятийный аппарат юридической науки дополняется такими терминами как «цифровое право», «цифровая идентичность», «цифровая безопасность», «цифровая свобода» и другими.

Рассматривая содержание понятия цифровой идентичности как базовой категории в цифровой среде, следует отметить, что термин «идентичность» в самом общем смысле означает свойство человека относить себя к какой-либо социальной группе в зависимости от определенного признака (пол, возраст, национальность, род занятий и т.д.). При этом, современное развитие информационно-коммуникационных технологий, а также их широкое использование во всех сферах жизни общества, позволяет говорить о новом виде идентичности - цифровой, которую А.В. Туликов рассматривает как уникальную совокупность информации о личности, представленной в цифровой форме, с использованием которой индивиды вступают в правоотношения, осуществляют права и обязанности [1, с. 28]. Более того, цифровую идентичность можно также рассматривать в качестве субъективного права, дающего возможность индивиду действовать в

цифровой среде от своего имени, либо используя вымышленное имя, либо анонимно. Наконец, цифровую идентичность можно обозначить как один из видов цифровых активов наряду с криптовалютой и токенами. Важной особенностью цифровой идентичности является ее отличие от идентичности реальной, так как участники общественных отношений в цифровой среде не всегда обязаны указывать достоверные данные о своей идентичности.

Наиболее актуальной проблемой реализации индивидом права на цифровую идентичность является тот факт, что в настоящее время она подвергается большому числу атак не только со стороны злоумышленников, стремящихся ее подделать, украсть, но и правительств, транснациональных корпораций и иных организаций. Большинство из рассматриваемых угроз цифровой идентичности связано с тем, что информация о личности, хранящаяся в цифровой форме, активно приобретает свойство товара, рыночная стоимость которого увеличивается с высокой скоростью.

Обладание информацией о цифровой идентичности может также стать инструментом для управления пользователями. Еще И. Бентам полагал, что в целях наилучшего управления обществом необходимо суммировать все удовольствия или страдания отдельной личности, информацию о которой сейчас можно добыть в цифровой форме [2, с. 161]. Несомненно, любому государству необходимо собирать и обрабатывать персональные данные своих граждан для решения большого числа управленческих задач, таких как обеспечение национальной безопасности, сбор налогов, охрана общественного порядка, осуществление социальных программ и другие. Вместе с тем следует обеспечивать защиту личности от незаконного вмешательства в ее личную жизнь, в том числе от посягательств на тайну корреспонденции, телефонных и иных сообщений, которые закреплены ст. 28 Конституции Республики Беларусь.

В связи с изложенным полагаем, что одной из самых актуальных остается проблема защиты пользовательских данных в цифровой среде, которая в Республике Беларусь обостряется тем, что в условиях несовершенства правового регулирования и защиты данных на наш рынок попадает большое число иностранной техники, программного обеспечения, которые получают доступ к личным данным граждан Республики Беларусь.

Одной из гарантий реализации и защиты цифровой идентичности может стать включение в национальное законодательство концепции, подобно той, что заложена в Генеральный регламент по защите данных в ЕС (Регламент 2016/679 Европейского парламента и Совета Европейского Союза от 24 октября 2016 года о защите прав

частных лиц применительно к обработке персональных данных и о свободном движении таких данных, и отменяющий Директиву 95/46/ЕС, далее – Регламент) – «проектируемой конфиденциальности» (privacy by design), согласно которой защита личной информации, не может быть обеспечена исключительно соблюдением нормативных правовых актов, правило, обеспечивающее защиту пользовательских данных, должно быть заложено в саму архитектуру программного обеспечения по умолчанию на протяжении всего цикла сбора, хранения, обработки и уничтожения информации. Кроме того, для достижения «проектируемой конфиденциальности» необходимо реализовать целый комплекс мер: защита личной информации по умолчанию; своевременное уведомление о сборе личной информации; предоставление пользователю свободы выбора в удобной и понятной форме. Названные меры могут сочетаться с обязательным требованием о том, что сбор, обработка и хранение пользовательских данных должны осуществляться с заранее определенной целью на основании конкретно выраженного свободного информированного однозначного согласия субъекта данных с возможностью его отзыва.

Изменения в действующем законодательстве при реформировании сложившихся подходов по защите персональных данных необходимы, прежде всего для того, чтобы вернуть пользователю контроль над своими данными. Техническим решением, по оценке специалистов, может стать использование технологии блокчейн, архитектура которой построена на законах экономики и математики и обладает рядом сравнительных преимуществ. Во-первых, рассматриваемая система децентрализована, что означает снижение рисков потери информации, а также ее изменения, во-вторых, безопасность в блокчейне обеспечивается средствами криптографической защиты, основанными на прозрачности и проверяемости всех манипуляций в системе, в-третьих, данная система позволяет осуществлять прозрачное использование данных. Однако проблемными могут стать вопросы определения данных в блокчейне, а также лица, их контролирующего, установления места обработки данных и соответствующей юрисдикции, масштабируемость системы. Более того, принятие некоторых законодательных положений может вступать в противоречие с архитектурой блокчейн систем. В частности, Регламент, о котором выше велась речь, содержит в себе положения о «праве на забвение», сформированного судебной практикой еще по делу испанского гражданина Марио Гонсалеса против Google [3]. Данное право можно рассматривать как возможность любого человека при определенных условиях потребовать у контролера данных удалить неполные, уста-

ревшие, неточные сведения о нем при условии, что нет никаких законных оснований для их сохранения. Вместе с тем, в отличие от централизованных сетей, которые выполняют операции создания, чтения, обновления, удаления информации, в публичном блокчейне данные не могут быть изменены либо удалены, кроме того отсутствует администратор, имеющий полномочия на данные операции.

Таким образом, цифровая среда нуждается в создании надежной системы, гарантирующей пользователям реализацию и защиту их прав, в том числе на сохранение цифровой идентичности. Базовым принципом может стать принцип проектируемой конфиденциальности, презюмирующий недостаточность соблюдения требований нормативных правовых актов при работе с персональными данными пользователей, который также требует от операторов по сбору, хранению и обработке данных создания надежной архитектуры используемых систем. При этом создание идентичности на основе архитектуры блокчейн систем позволит индивидам иметь возможность контролировать доступ к их персональным данным.

Библиографические ссылки

1. Туликов, А.В. Информационная безопасность и права человека в условиях постиндустриального развития: (теоретико-правовой анализ): диссертация на соискание ученой степени кандидата юридических наук: специальность 12.00.01 / А.В. Туликов; [Национальный исследовательский университет «Высшая школа экономики»] – Москва, 2017. – 180 с.

2. Кин, Э. Ничего личного: как социальные сети, поисковые системы и спецслужбы используют наши персональные данные / Э. Кин. – М: Альпина Паблишер Sferiq, 2016. – 220 с.

3. An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties: Press release № 70/14 // Court of Justice of the European Union [Electronic resource]. – Mode of access: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> – Date of access: 13.02.2018.

СПОРТИВНАЯ ДИСКВАЛИФИКАЦИЯ ЗА ДОПИНГ КАК МЕРА ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ

Мороз Владимир Петрович,

заместитель директора учреждения образования «Институт переподготовки и повышения квалификации судей, работников прокуратуры, судов и учреждений юстиции Белорусского государственного университета» (г. Минск), кандидат юридических наук, доцент
morozv@bsu.by

Развитие в последние годы спортивного права со всей очевидностью обнаружило важность его проблематики в целом и сложность связанных со спортом специфических вопросов, в частности, такого