ный сайт Прокуратуры Республики Башкортостан. 2023. 31 августа. [Электронный ресурс]. URL: https://epp.genproc.gov.ru/web/proc_02/mass-media/news/archive?item=89957211 (дата обращения: 10.07.2024).

12. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=m0s68mbuop17134260 (дата обращения: 10.07.2024).

13. Антонова Е. Ю. Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию. Journal of Digital Technologies and Law. 2023. № 1(1). С. 251–269. DOI: https://doi.org/10.21202/jdtl.2023.10 ; EDN: HFPMTN

Н. Н. Бойко,
кандидат юридических наук, доцент,
Уфимский университет науки и технологии,
Стерлитамакский филиал

РАССМОТРЕНИЕ ВОПРОСОВ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Статья посвящена исследованию проблем, связанных с обеспечением информационной безопасности. Круг исследуемых правоотношений является относительно новым явлением в российском правовом поле, в связи с чем они надлежащим образом не урегулированы нормами отечественного права. Кроме того, данные отношения развиваются стремительно, что обуславливает необходимость оперативного реагирования на новшества в сфере информационной безопасности. Необходимость в обеспечении информационной безопасности очерчена в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Президентом России. В силу того, что количество угроз в рассматриваемой сфере выросло, предлагается их классификация, что позволит выработать более эффективные меры по борьбе с данными явлениями.

Ключевые слова: право, цифровые технологии, интернет-технологии, информационное общество, информационная безопасность, угрозы информационной безопасности, кибербуллинг, несовершеннолетние, обеспечение безопасности личности

CONSIDERATION OF LEGAL SUPPORT ISSUES INFORMATION SECURITY

Abstract. The present article is devoted to the study of problems related to the provision of information security. The range of legal relations under study is a

relatively new phenomenon in the Russian legal field, therefore they are not properly regulated by the norms of domestic law. In addition, these relations are developing rapidly, which necessitates a prompt response to innovations in the field of information security. The need to ensure information security is outlined in the Strategy for the Development of Information Society in the Russian Federation for 2017–2030, approved by the President of Russia. Due to the fact that the number of threats in this area has increased, the author proposes their classification, which will allow to develop more effective measures to combat these phenomena.

Keywords: law, digital technologies, Internet technologies, information society, information security, threats to information security, cyberbullying, minors, personal security

Введение. Широкое развитие информационных технологий привело к тому, что они охватили все сферы жизнедеятельности человека, а также государства. Данное обстоятельство связано с тем, что технологии открывают новые возможности, решают проблемы, связанные с коммуникацией между различными субъектами, упрощает многие операции, а также повышает производительность работы всех ведомств и учреждений. Государство активно поддерживает внедрение новых технологий в различные органы и учреждения, выделяя денежные средства, а также обеспечивая различными социальными гарантиями IT-специалистов.

Основная часть. Цифровизация общества и государства привела к тому, что информационные технологии стали неотъемлемым элементом нашей культуры, создавая новые ценности в обществе и стандарты взаимосвязи между различными субъектами общественных отношений [1].

Между тем, обретая столь важное значение и место в обществе, общественные отношения в исследуемой сфере нуждаются в должном правовом регулировании. Традиционные проблемы общества, такие как преступность, построение общения между обществом и государством, социальное расслоение между различными классами общества, плавно перешли и в цифровое пространство. Более того, цифровизация общества наделила их новыми атрибутами, что требует от государства новых решений обозначенных проблем.

Для разрешения проблем, связанных с информационными технологиями, была разработана соответствующая концепция информационной безопасности, обозначенная в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы.

Исходя из содержания данного акта и анализа обозначенных угроз информационной безопасности, считаем, что их можно разделить на две группы:

– во-первых, угрозы, связанные с незаконным доступом к информации. В данном случае информация может носить конфиденциальный характер, и она не должна стать достоянием третьих лиц. Это могут быть сведения из личной или деловой переписки, информация, связанная с охраняемой законом тайны, личные фотографии и видеозаписи;

– во-вторых, угрозы, связанные с нарушением требований непосредственно к информации. В данном случае речь может идти о недостоверной (ложные све-

дения об угрозах безопасности граждан) или вредоносной (материалы порнографического характера, демонстрация фильмов с рейтингом 18+ несовершеннолетним и т. п.) информации.

Информация может носить открытый и ограниченный характер. В последнем случае информация может быть запрещена полностью (информация о местах продажи наркотических веществ, огнестрельного оружия, военная тайна и т. п.) либо частично (разрешена для взрослых лиц, запрещена для детей).

Отдельно также следует рассмотреть проблему общения в сети Интернет. Осознавая факт того, что лица, участвующие в переписке, находятся на разных концах России, а также что личность переписывающихся зачастую не идентифицируется, пользователи часто ведут себя агрессивно и неадекватно с другими собеседниками. Споры и ссоры нередко перетекают в угрозы, а оскорбления и издевательства порой затрагивают расовую, национальную и религиозную принадлежность собеседника. Часто жертвами подобных провокаций и оскорблений становятся дети, которые в силу особенностей своего психического развития могут более болезненно воспринимать данные негативные явления.

Для защиты детей от негативной информации Федеральным Собранием РФ был принят ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», однако он не решил многих проблем, едва коснувшись лишь информации, которая публикуется в СМИ.

К проблемам, связанным с защитой прав детей в информационно-телекоммуникационных сетях, можно отнести следующие:

1) кибербуллинг – оскорбления в сети Интернет, распространение недостоверных сведений или сведений, которые носят характер личной тайны, а также различного рода провокации [5. P. 99]. Как уже было сказано, дети могут крайне чувствительно реагировать на подобного рода действия. Они могут уйти в себя, бросить заниматься учебой или увлечением и в худшем случае совершить самоубийство [4. P. 183]. В настоящее время дети часто подвергаются травле со стороны взрослых за новое увлечение – квадробинг. Разумеется, данное увлечение может вызывать определенную обеспокоенность, однако это не является поводом оскорблять и унижать их;

2) размещение в сети Интернет информации, не предназначенной для детского просмотра. Интернет-провайдеры активно предпринимают усилия для недопущения размещения на платформах, которыми пользуются в том числе и дети, запрещенной или ограниченной в пользовании информации, однако полностью оградить детей от этого фактически невозможно. Кроме того, часто дети «проникают» в интернет-ресурсы, где не должны находиться. Подобные интернет-ресурсы часто формально подходят к вопросу ограничения доступа детей к своему контенту. Либо же это лишь предупреждение о размещении запрещенного контента, либо незамысловатая система регистрации, где достаточно указать в анкете ложные сведения о своем возрасте;

3) информация, вводящая в заблуждение детей. Дети, в силу отсутствия жизненного опыта, знаний и личной наивности, легко могут быть введены в заблуждение. Речь идет не только о различных формах интернет-мошенничества, которое заполонило все цифровое пространство. Это может быть реклама бесплатных онлайн-игр, где необходимо за реальные деньги приобретать товары для

игры, различные способы интернет-заработка и т. д. Законодательство европейских стран запрещает игровым издателям выпускать игры для детей с элементом азартных игр, а также такие, где необходимо регулярно делать платежи реальными деньгами. Отечественное законодательство никаких ограничений в этом плане не создает;

4) угроза сексуального насилия в отношении детей. Несмотря на то, что сексуальное насилие подразумевает физический контакт с потерпевшим, угрозу для психического и нравственного развития могут иметь и интернет-формы сексуального насилия. Нередко лица, имеющие сексуальные девиации, отправляют потерпевшим сцены сексуального насилия над детьми, животными, умершими; непристойные предложения; требуют отправить фотографии интимного характера. Будучи уверенными в своей безнаказанности и анонимности, данные лица все изощреннее ведут в себя социальных сетях [3. С. 363]. В данном случае проблема заключается в том, что отечественное законодательство не регулирует вопрос этики общения в сети Интернет на подобные темы. Сексуальное домогательство в своем легальном понимании подразумевает «живое» общение на подобные темы, в связи с чем достаточно сложно привлечь к ответственности лиц за подобного рода действия в сети Интернет;

5) нарушение конфиденциальности данных несовершеннолетних. Российское законодательство запрещает размещать персонифицированную информацию о детях, ставших жертвами преступлений, а также данные личного характера, сведения о тайне усыновления, медицинские данные и т. п. Однако часто СМИ данные требования игнорируют либо по своей невнимательности забывают деанонимизировать детей, ставших жертвами сексуального насилия.

Заключение. Таким образом, законодательство об информационной безопасности требует серьезной модернизации, особенно если речь идет о несовершеннолетних пользователях. При этом нельзя сводить все меры к запрету и ограничению, поскольку подобного рода меры показывают крайнюю неэффективность. Отношения в исследуемой сфере требуют более точечного подхода. Невозможно полностью огородиться в сети Интернет от нежелательной информации. В определенных случаях необходимо требовать от владельцев интернет-ресурсов проведения более оперативной модерации поступающей информации, в других случаях необходимо проработать меры ответственности за нарушение этики общения в сети Интернет. Также следует проводить воспитательные мероприятия с детьми и их родителями для выработки «иммунитета» от кибербуллинга и действий различных мошенников. Также считаем необходимым обязать интернет-ресурсы ввести в будущем специальный искусственный интеллект, который будет автоматически выявлять случаи нарушения законодательства об информационной безопасности и предпринимать меры по устранению данных нарушений и при необходимости собирать информацию о злостных нарушителях.

Список литературы

1. Анненкова И. В., Залоило М. В. Новая культура коммуникаций в условиях цифровой и социокультурной глобализации: право, медиа и национальная идентичность // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. С. 140–155.

2. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29.12.2010 № 436-ФЗ (последняя редакция) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_108808 (дата обращения: 05.09.2024).

3. Филиппов В. М., Насонкин В. В., Папачараламбоус Ч. Права и интересы детей в информационной сфере: реформирование законодательства // Вестник Санкт-Петербургского университета. Право. 2019. Т. 2, № 2. С. 362–372.

4. Payyz M. A. O regulirovanii psikhicheskogo nasiliya normami UK RK [On the regulation of mental violence by the norms of the Criminal Code of the Republic of Kazakhstan] // Nauchnyye trudy YUKGU im. M.Auezova. 2021. № 1(57). Pp. 183–189.

5. Zhumabekova K. Topical issues of protecting children from cyberbullying // Journal of actual problems of jurisprudence. 2022. Vol. 104, № 4. Pp. 98–103.

И. И. Брянцев,
кандидат социологических наук, доцент,
Поволжский институт управления имени П. А. Столыпина –
филиал Российской академии народного хозяйства и государственной
службы при Президенте Российской Федерации,
О. В. Брянцева,
кандидат физико-математических наук, доцент,
Саратовская государственная юридическая академия

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ЦИФРОВОЙ СРЕДЫ: ОБЩИЕ ТРЕНДЫ И РЕГИОНАЛЬНАЯ СПЕЦИФИКА

Аннотация. Цифровые информационные инструменты стали неотъемлемой частью системы сбора, хранения, обработки и передачи как уже имеющихся, так и только появляющихся знаний в сфере государственного и муниципального управления. Это обуславливает актуальность использования этих инструментов для повышения эффективности работы государственных органов, ускорения процессов принятия решений, обеспечения прозрачности и транспарентности публичной власти. В статье представлены результаты анализа региональных практик и особенностей формирования правовой среды и реализуемых организационных мер, обеспечивающих динамичное развитие цифровой среды.

Ключевые слова: право, цифровые технологии, цифровая трансформация, цифровая среда, государственные услуги, органы публичной власти, общественный контроль

ORGANIZATIONAL AND LEGAL ASPECTS OF THE FORMATION OF THE DIGITAL ENVIRONMENT: GENERAL TRENDS AND REGIONAL SPECIFICITY

Abstract. Digital information tools have become an integral part of the system for collecting, storing, processing and transmitting both existing and emerging knowledge in the field of public and municipal administration. This determines the