
Права человека в условиях цифровизации общества

Чернышева Ю.А., кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики ФГБОУ ВО «Елецкий государственный университет имени И.А. Бунина» (E-mail: lavytrans@mail.ru)

Целью научной работы является комплексное теоретико-правовое исследование содержания и особенностей, проблем реализации прав человека в условиях цифровизации общества и разработка на этой основе научно-обоснованных рекомендаций, действенных механизмов, направленных на эффективную защиту прав и свобод человека в современной России.

Методологическую основу исследования представляют общенаучный диалектический метод и комплекс научных методов познания (формально-юридический, системно-структурный, формально-логический).

Результаты, к которым пришел автор, говорят о том, что на современном этапе развития нашего общества от государства требуется защита прав и интересов человека в условиях глобальной цифровизации. Законодатель должен определить формы оборота информации; установить права и обязанности участников «цифровых» правоотношений; пределы применения цифровых технологий и многое другое.

В заключение сформулирован вывод о том, что развитие информационных технологий сопровождается злоупотреблением ими в преступных целях, а также подчеркивается необходимость разработки правовых мер по противодействию правонарушениям и преступлениям в области цифровизации всех сфер жизнедеятельности нашего государства.

Ключевые слова: цифровизация общества, «цифровые права», квалифицированная электронная подпись, информационная безопасность, «электронное правительство», система идентификации и аутентификации, персональные данные, электронное правосудие, право цифровых денег, программное право, право цифровых споров.

Для цитаты:

Чернышева Ю.А. Права человека в условиях цифровизации общества. [Электронный ресурс] // Психология и право. 2019 (9). № 4. С. 90-102. doi: 10.17759/psylaw.2019090407

For citation:

Chernysheva Yu.A. Human rights in a digitalized society. [Elektronnyi resurs]. Psikhologiya i

pravo [Psychology and Law], 2019(9), no. 4. pp.90-102.
doi: 10.17759/psylaw.2019090407

I. Введение

Проблема обеспечения и защиты прав человека сложна, комплексна и динамична. Права человека развиваются, обогащаются, их состав и содержание расширяются под воздействием различных факторов. Причем если некоторые факторы действуют эволюционно, то Интернет способствует гораздо более ощутимым изменениям права в целом и прав человека в частности [5, с. 117—149].

Российская Федерация является демократическим правовым государством, где за долгие годы реформ были созданы условия для формирования гражданского общества, признающего человека, его права и свободы высшей ценностью [2, с. 4—5].

Основные права человека, гарантированные Конституцией РФ и международно-правовыми актами, варьируются законодательством в зависимости от определенного исторического этапа развития страны. Законодатель при этом должен обеспечить оптимальный уровень конкретизации конституционных прав и свобод.

Цифровизация жизни граждан постепенно привела к появлению «цифровых прав», под которыми В. Зорькин предлагает понимать «...права граждан на доступ, использование, создание и публикацию цифровых произведений, на доступ и использование компьютеров и иных электронных устройств, коммуникационных сетей и сети Интернет, а также право свободно общаться и выражать свое мнение в Сети и право на неприкосновенность частной информационной сферы, включая право на конфиденциальность, анонимность его оцифрованной персональной информации» [1].

Эпоха информационных технологий диктует необходимость ревизии универсальных прав человека и их расширения. Сегодня одной из основных задач государства является признание и защита цифровых прав граждан от возможных нарушений с одновременным обеспечением конституционно-правовой безопасности личности, общества и государства на основе Конституции и с учетом необходимых международных документов.

При внедрении в жизнь современных цифровых технологий при широком декларировании Конституцией РФ прав и свобод человека и гражданина юридическая незащищенность индивидуума остается очевидной. Существующая на сегодняшний день ситуация требует разработки концепции по развитию системы российского законодательства в области защиты прав человека в сфере цифровых технологий.

Защите прав человека в цифровую эпоху посвятили свои труды Зорькин В., Коршунова О.Н., Ломакин А., Талапина Э.В. и др.

О проблеме конкретизации права в условиях цифровизации общественной практики пишет в своей работе Степанов О.А.

Вопросам применения информационных технологий посвящено достаточно большое количество трудов на международном уровне: Pachis J.A., Zonneveld K.L.M., Mertens A., Schäfer

K., Rasche P., Bröhl C., Theis S., Seinsch T., Brandl C., Wille M., Jovanović M., Dlačić J., Okanović M. и др.

Anderson C., Baskerville R.L., Kaul M. в своей работе акцентировали внимание на выработке политики информационной безопасности, защите прав человека.

2. Методология

В настоящей работе использован общенаучный диалектический метод, а также формально-юридический, системно-структурный, формально-логический методы познания.

Общенаучный диалектический метод дал возможность комплексно исследовать сущность прав человека в условиях развития цифровых технологий, проанализировать наиболее важные проблемы защиты прав, возникших на современном этапе развития общества, сформулировать предложения, которые могут способствовать созданию наиболее продуманной и эффективной системы защиты прав человека.

При анализе действующего законодательства РФ использовался формально-юридический метод.

С помощью системно-структурного метода описано и проанализировано правовое обеспечение реализации прав в условиях цифровизации социальной жизни общества.

Формально-логический метод помог обратиться к уже существующим формам мышления и логическим законам при выявлении пробелов в действующем законодательстве.

3. Результаты исследования

В широком смысле под цифровизацией можно понимать современный общемировой тренд развития общества и экономики, который основан на преобразовании информации в цифровую форму и приводит к повышению эффективности экономики и улучшению качества жизни.

К цифровым правам человека относятся право на публикацию цифровых произведений, право на использование компьютеров и других электронных устройств. Подотраслями цифрового права являются авторское и программное право, право цифровых денег и цифровых споров, право доступа к различным данным и защиты при доступе и др. Данные права могут быть нарушены со стороны государства правоохранительными органами, а также Интернет-провайдером при навязывании цифровых услуг.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» одним из основных цифровых прав граждан считает конфиденциальность и анонимность персональной информации. Под защитой государства находятся цифровые права граждан и организаций, например, в области применения соответствующего законодательства об информации, информационных технологиях и о защите информации. Как физические, так и юридические лица могут осуществлять поиск и получать информацию в любых формах и из любых источников, но только при соблюдении требований закона. Также они могут получать от государственных органов информацию, затрагивающую их права и

обязанности, а государственные органы и органы местного самоуправления должны предоставить доступ к информации о своей деятельности.

Информацию необходимо предоставлять в форме электронного документа, который подписывается усиленной квалифицированной электронной подписью, и (или) документа на бумажном носителе. Юридические и физические лица предоставляют государственным органам информацию в форме электронных документов, подписанных электронной подписью, если иное не установлено законом [3, с. 65—74].

Данное взаимодействие регламентируется Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [7]

С начала 2017 г. действуют поправки в гражданское, уголовное административное законодательство о том, что участники судебного производства могут направлять в суд документы и доказательства по делу в электронном виде, подписанные электронной подписью через сайт суда. Необходимо также создать аккаунт на Портале государственных услуг для того, чтобы можно было зайти в свою учетную запись в информационной системе для подачи документов в суд.

Согласно новым поправкам, в электронном виде могут быть представлены и судебные решения, подписанные усиленной квалифицированной электронной подписью, за исключением особой категории дел.

Недавно вступил в силу законопроект, который предусматривает онлайн-трансляции судебных заседаний и устанавливает сроки размещения судебных актов в сети Интернет.

При внедрении данной системы будет обеспечена доступность правосудия для общества, но при этом не стоит забывать о безопасности в сохранности информации через защиту логина пользователя личным паролем на сайте Госуслуг и подписание документов личной электронной подписью. С каждым днем растет число личных кабинетов в сервисе «Электронное правосудие», а также увеличивается объем документов, поступающих в электронном виде в суды.

К отрицательным сторонам электронного документооборота необходимо отнести то, что часть текстов судебных актов не публикуются или появляются на судебных сайтах несвоевременно.

Необходимо сказать и об Электронном правительстве, т.е. пакете технологий и наборе сопутствующих мер, нормативно-правового обеспечения для осуществления цифрового обмена между органами государственной власти, гражданами, организациями и другими субъектами экономики.

Главными задачами программы российской модели электронного правительства являются повышение эффективности функционирования экономики, государственного и местного управления, создание условий для свободного доступа к информации и получения необходимых услуг.

Необходимо отметить, что сегодня в нашей стране работает единая информационная система идентификации и аутентификации (ЕСИА), которая обеспечивает доступ граждан-заявителей и должностных лиц к информации, содержащейся в государственных и иных

информационных системах. С ее помощью проходит авторизация на сайте Российской общественной инициативы и на Портале госуслуг.

Российская общественная инициатива (РОИ) – это Интернет-ресурс, при помощи которого граждане Российской Федерации, авторизованные через ЕСИА, вправе выдвигать различные гражданские инициативы или голосовать за них [3, с. 65—74].

Государство предпринимает меры по защите информации от неправомерного доступа, изменения, уничтожения, блокировки, копирования, предоставления или распространения, а также от других неправомерных действий. Закон предусматривает дисциплинарную, гражданско-правовую, административную и уголовную ответственность.

К основным вопросам информационной безопасности государства относятся защита информации, сохранность информации, а также реализация гарантий конституционных прав и свобод гражданина, касающихся деятельности в информационной сфере.

Государство, в целях защиты информации, обеспечивает гражданам, кроме гарантированных Конституцией РФ прав и свобод, право на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых и других сообщений, защиту чести и достоинства. Необходимо заботиться и о повышении безопасности информационных систем государственных органов, финансовой и банковской отраслей, а также о защите сведений, составляющих государственную тайну.

Если говорить о правоотношении физических, юридических лиц и государства, необходимо отметить, что Федеральный закон 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и защите информации» гласит, что «...информационные ресурсы подлежат обязательному учету и защите как материальное имущество собственника» [8].

Законодательство рассматривает заключение гражданско-правовых договоров или оформление иных правоотношений, где происходит обмен электронными сообщениями, подписанными электронной подписью, как обмен документами.

С точки зрения права выделяется информация без ограниченного права доступа и информация с ограниченным доступом (коммерческая, государственная, банковская, профессиональная тайна и персональные данные), запрещенная к распространению информация, объекты интеллектуальной собственности и прочая информация.

Незаконное засекречивание, нарушение содержания предоставляемых сведений, неопубликование сведений, нарушение прав граждан на бесплатное получение информации, непредоставление сведений об обстоятельствах, создающих опасность для жизни или здоровья людей, искажение или несвоевременное предоставление сведений, сокрытие информации или сообщение о недостоверных сведениях и в других случаях предусматривает ответственность по закону.

Защита права лица на доступ к информации происходит путем направления жалобы на должностное лицо или государственный орган в Судебную палату по информационным спорам при Президенте РФ или путем представления искового заявления или жалобы для рассмотрения в гражданском, административном или уголовном судопроизводстве.

Необходимо отметить, что помимо информационной безопасности государства, существует и информационная безопасность предприятия. Каждое предприятие заинтересовано в защите корпоративных сведений, сохранении их конфиденциальности [3, с. 65—74].

Принципиально новые возможности использования цифровых технологий открываются и для оптимизации государственных функций на основе конституционных принципов верховенства права и народовластия.

В скором времени IT-технологии позволят с помощью программного кода обеспечить однозначность содержания законов и нормативных правовых актов. Сторонники подобных разработок пока преувеличивают возможности кодирования и недооценивают вариативность общественных отношений, подлежащих регулированию. В настоящее время возникла потребность создания благоприятных условий для безопасного функционирования информационных систем.

Повсеместная цифровизация создала необходимость развития эффективного механизма защиты частной жизни человека и гражданина, включая обработку персональных данных.

Активное внедрение средств обеспечения безопасности и достоверности операций требует дальнейшего совершенствования.

Применение современных информационных технологий требует от законодателя определения форм оборота информации, установления прав и обязанностей участников «цифровых» правоотношений, пределов применения цифровых технологий и многое другое.

4. Обсуждение

В последние годы практически все государства, а также межгосударственные объединения и организации уделяют значительное внимание проблемам цифровизации. Анализ их актов создает достаточно целостную картину, адекватно отражающую мировые процессы.

Известно, что в европейских странах право на защиту персональных данных «выводится» из права на защиту частной жизни [12, с. 135—153]. Право на частную жизнь — одна из азбучных истин континентального права [21, с. 19]. Например, французская доктрина различает две составляющие частной жизни — личная частная (персонально-интимная) жизнь и социальная частная жизнь. Именно в логику социальной частной жизни отлично вписываются социальные сети, в то время как с личной частной жизнью они скорее находятся в антагонистических отношениях. Европейский суд по правам человека подтвердил право любого индивида строить отношения с другими людьми, охватив впоследствии этим правом и электронную переписку. Директива Европейского парламента и Совета Европейского союза от 15 декабря 1997 г. № 97/66/ЕС [13, с. 1—8], касающаяся обработки персональных данных и защиты неприкосновенности частной жизни в области телекоммуникации, обязывает «...государства на уровне национального законодательства обеспечивать конфиденциальность коммуникаций, осуществляемых посредством общедоступной телекоммуникационной сети и общедоступных телекоммуникационных услуг» (п. 1 ст. 5). Все это — право на частную жизнь.

В определенной мере данная «связка» частной жизни и персональных данных используется и на более высоком уровне — в деятельности Организации Объединенных Наций. Так, 24.03.2015 г. Комитет по правам человека принимает решение об учреждении на трехлетний период должности Специального докладчика по вопросу о праве на неприкосновенность частной жизни, в сферу компетенции которого входит и защита персональных данных. Этому предшествовал доклад Верховного комиссара ООН по правам человека о праве на неприкосновенность личной жизни в цифровой век (30 июня 2014 г.). В докладе подчеркивается, что государство как таковое обеспечивает охрану частной жизни, соблюдение прав человека. Но исходя из разделения ответственности с частным сектором, определенные обязательства несут и бизнес-структуры. В частности, на их уровне должна обеспечиваться защита персональных данных. Заметим, что различается защита персональных данных вообще и защита данных при автоматизированной обработке [5, с. 117—149].

Поскольку в правовом пространстве России действуют, как правило, правовые нормы общего характера, потребность в конкретизации их содержания в современных условиях обусловлена необходимостью учета технологических особенностей цифровизации. Вместе с тем на современном этапе теоретического осмысления данной проблемы, юридическая наука отстает от потребностей юридической практики. Так, в должной мере проблема конкретизации права применительно к сфере цифровизации сетей и технологий, связанная с противодействием терроризму, пока не изучена ни на теоретическом, ни на практическом уровне.

Переход на электронное управление технологическими процессами в производстве, по мнению российских и зарубежных экспертов, является предпосылкой террористических действий с использованием информационно-телекоммуникационных сетей. По оценкам ФСБ России, подготовка всех террористических атак на территории России в 2017 г. координировалась через мессенджеры. Такие действия вполне объективно подпадают под ст. 205 УК РФ [6], в соответствии с которой «... совершение действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями», т.е. террористические деяния с использованием информационно-телекоммуникационных сетей носят характер «иных действий», что является достаточным для правовой квалификации таких действий.

При рассмотрении конкретизации как фактора придания праву (в субъективном смысле) максимальной определенности в процессе правоприменительной деятельности следует обратить внимание и на систему взглядов на угрозы в сфере компьютерной информации [4, с. 4—23].

Исследование наиболее актуальных проблем, возникающих при применении современных информационных средств, позволило обосновать необходимость совершенствования норм российского законодательства. Учитывая важность соблюдения прав человека в современном мире, мы считаем, что опасность для общества и государства посягательств на права человека в области цифровизации диктует необходимость их

криминализации, а также разработки мер по предупреждению подобного рода преступлений и правонарушений.

5. Заключение

Общество сегодня живет в новой цифровой реальности, созданной информационными технологиями [1]. Цифровые технологии проникли во все сферы деятельности человека и уже сегодня идет речь о создании новой реальности, которая не будет иметь аналогов в прежнем мире. Цифровизация общества, его политической и экономической составляющих говорит о том, что назрела необходимость наполнения национальных правовых систем стандартами, которые приобретут иную степень совместимости в рамках формирования макросреды правового регулирования [4, с. 4—23].

Задачей государства является защита цифровых прав граждан от различных нарушений, но существующее сегодня законодательство не в полной мере отвечает современным реалиям. Поэтому законодательство, касающееся регулирования цифровых прав граждан, нуждается в модернизации и систематизации, приведении его понятийного аппарата в стройное, непротиворечивое состояние [1].

Важной проблемой взаимоотношения власти и гражданина в цифровом обществе является определение возможных ограничений цифровых прав федеральным законом, в том числе допустимых пределов контроля информационной среды со стороны правоохранительных служб с целью обеспечения эффективной защиты общества от киберпреступлений. Поэтому необходим поиск оптимального правового компромисса между возможностью доступа правоохранительных служб к компьютерной информации и правом граждан на ее конфиденциальность.

Методологическим ориентиром и отправной точкой здесь должны стать конституционные принципы и нормы. Независимо от того, насколько сегодня развита цифровая реальность, она должна подпадать под действие Конституции РФ как нормативного акта, имеющего высшую юридическую силу в правовой системе России, в том числе по отношению к законоположениям, регулирующим рассматриваемую сферу новых отношений.

Все сказанное говорит о том, что сегодня необходим поиск оптимального правового компромисса между возможностью доступа спецслужб и правоохранительных органов к компьютерной информации и правом граждан на ее конфиденциальность [1].

Сегодня в любом государстве можно наблюдать нарушение прав человека и гражданина. Не соблюдается тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, нарушаются свобода слова и печати, права авторов и изобретателей и другие конституционные права и свободы.

Общий объем преступлений и правонарушений против конституционных прав и свобод человека, совершаемых в Российской Федерации в сфере цифровых технологий, из года в год возрастает.

Актуальность вопроса защиты прав человека в условиях развития информационного общества заключается, прежде всего, в отсутствии целостной концепции правовых мер противодействия посягательствам на права человека и недостаточного законодательного

регулирования и единообразного понимания правовых норм в доктрине и правоприменительной практике.

Литература

1. Зорькин В. Право в цифровом мире // Российская газета: Столичный выпуск. №7578 (115).
2. Коршунова О.Н. Защита прав человека в современном демократическом государстве: дисс. ... канд. юр. наук. М., 2008. 170 с.
3. Ломакин А. Цифровизация права // Трудовое право. 2017. № 9. С. 65—74.
4. Степанов О.А. О проблеме конкретизации права в условиях цифровизации общественной практики // Право. Журнал Высшей школы экономики. 2018. № 3. С. 4—23.
5. Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. 2018. № 5. С. 117—149.
6. Уголовный кодекс РФ от 13 июня № 63-ФЗ // Российская газета от 18 июня 1996 г. № 113, 114, 115, 118.
7. ФЗ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Российская газета от 8 апреля 2011 г. № 75.
8. ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и защите информации» // Российская газета от 29 июля 2006 г. № 165.
9. Anderson C., Baskerville R.L., Kaul M. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information // Journal of Management Information Systems. 2017. Vol. 34. Iss. 4. P. 1082—1112. doi:10.1080/07421222.2017.1394063.
10. Baskerville R. Information security: Going digital (invited lecture) // Communications in Computer and Information Science. 2019. Vol. 963. P. 3. 1447 th Annual Conference of the Southern African Computing Lecturers Association, SACLA 2018; Gordon's Bay; South Africa; 18 June 2018 до 20 June 2018. doi: 10.1007/978-3-030-05813-5_1.
11. Burukina O., Karpova S., Koro N. Ethical Problems of Introducing Artificial Intelligence into the Contemporary Society // Advances in Intelligent Systems and Computing. 2019. Vol. 876. P. 640-6461. doi: 10.1007/978-3-030-02053-8_98.
12. Bouhadana I. The right to the respect of privacy in digital age in the French law system // Эволюция государственных и правовых институтов в условиях развития информационного общества / Сборник научных работ. М.: ИГП РАН, юридическое издательство «ЮРКОМПАНИ», 2012. С. 135—153.
13. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the

telecommunication sector // OJ. L 24. 30 January 1998. Vol. 41. P. 1—8.

14. *Dneprovskaya N.V., Bayaskalanova, T.A., Ruposov, V.L., Shevtsova, I.V.* Study of Digitization of Russian Higher Education as Basis for Smart Education // Proceedings of the 2018 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2018 5 November 2018, Номер статьи 8524945, Pages 607-611 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2018; St. Petersburg; Russian Federation; 24 September 2018 до 28 September 2018; Номер категории CFP18J17-ART; Код 142117. doi: 10.1109/ITMQIS.2018.8524945.
15. *Frolova E.E., Polyakova, T.A., Dudin, M.N., Rusakova, E.P., Kucherenko, P.A.* Information security of Russia in the digital economy: The economic and legal aspects // Journal of Advanced Research in Law and Economics. Spring 2018. Vol. 9. Iss. 1. P. 89—95. doi: 10.14505/jarle.v9.1(31).12.
16. *Heaton J., Parlikad, A.K.* A conceptual framework for the alignment of infrastructure assets to citizen requirements within a Smart Cities framework // Cities Volume 90, July 2019. P. 32-41. doi 10.1016/j.cities.2019.01.041
17. *Isa W.M.W., Zin, N.A.M., Rosdi, F., Sarim, H.M.* Digital preservation of intangible cultural heritage // Indonesian Journal of Electrical Engineering and Computer Science Volume 12, Issue 3, December 2018. P. 1373—1379. doi: 10.11591/ijeecs.v12.i3.pp1373-1379.
18. *Jovanović M., Dlačić, J., Okanović, M.* Digitalization and society's sustainable development — Measures and implications.[Digitalizacija i održivi razvoj društva — Mjere i implikacije] // Zbornik Radova Ekonomskog Fakultet au Rijeci Volume 36, Issue 2, December 2018. P.905—928. doi: 10.18045/zbefri.2018.2.905.
19. *Mertens A., Schäfer, K., Rasche, P., Bröhl, C., Theis, S., Seinsch, T., Brandl, C., Wille, M.* Shaping Ethical, Legal and Social Implications of the Digital Revolution Through Participation: The New Interdisciplinary Research Paradigm of Aachener DenkfabrEthik // Advances in Intelligent Systems and Computing Volume 824, 2019, Pages 1493-1497 20th Congress of the International Ergonomics Association, IEA 2018; Florence; Italy; 26 August 2018 до 30 August 2018; Код 216789. doi: 10.1007/978-3-319-96071-5_152.
20. *Pachis J.A., Zonneveld K.L.M.* Comparison of prompting procedures to teach internet skills to older adults // Journal of Applied Behavior Analysis. Vol.52. Iss. 1, Winter 2019, Pages 173—187. doi: 10.1002/jaba.519
21. *Pailler L.* Les ryeaux sociaux sur Internet et le droit au respect de la vie privye. Bruxelles, 2012. P. 19.
22. *Sousa M.J., Rocha Á.* Digital learning: Developing skills for digital transformation of organizations // Future Generation Computer Systems. February 2019. Vol.91. P. 327—334. doi: 10.1016/j.future.2018.08.048.

Human Rights in a Digitalized Society

***Chernysheva Y.A.,** Candidate of Law, Associate Professor of the Department of Criminal Procedure and Criminology Elets State University I.A. Bunina, Elets, Russia (lavytrans@mail.ru)*

The article focuses on a comprehensive theoretico-legal study of the content, features and problems of human rights realization in the context of digitalization of society as well as on following development of evidence based recommendations, practical mechanisms aimed at the viable defence of human rights and freedoms in modern Russia.

The methodological basis of the study is represented by the general scientific dialectic method and a set of scientific methods of understanding (technical, systemic structural, aristotelian method).

The results show that at the current stage of the development of society, the state is required to protect human rights and interests in the context of global digitalization. The legislator should determine the forms of information turnover; establish the rights and duties of participants in "digital" legal relations; the limits of digital technology application.

It is concluded that the development of information technology is accompanied by the abuse of such means for criminal purposes, and also emphasizes the development needs of legal measures to counter offenses and crimes in the field of digitalization of all areas of society.

Keywords: digitalization of society, digital rights, qualified electronic signature, information security, electronic government, identification and authentication system, personal data, e-justice, digital money law, software law, digital disputes law.

References

1. Zor'kin V. Pravo v tsifrovom mire [Right in a digital world] *Rossiiskaya gazeta - Stolichnyi vypusk*. [the Russian newspaper - Capital release], №7578 (115).
2. Korshunova O.N. Zashchita prav cheloveka v sovremennom demokraticheskom gosudarstve: Diss ... kand. jur. nauk. [Protection of human rights in a modern democratic state]. Moscow, 170 s.
3. Lomakin A. Tsifrovizatsiya prava [Digitalization of law]. *Trudovoe pravo*. [Labor law], № 9. 2017. S. 65-74.
4. Stepanov O.A. O probleme konkretizatsii prava v usloviyakh tsifrovizatsii obshchestvennoi praktiki [On the problem of concretization of law in the conditions of digitalization of public practice]. *Pravo. Zhurnal Vysshei shkoly ekonomiki*. [Journal of Higher School of Economics], 2018.S. 4-23.
5. Talapina E.V. Zashchita personal'nykh dannykh v tsifrovuyu epokhu: rossiiskoe pravo v evropeiskom kontekste [Protection of personal data in the digital age: Russian law in the European context]. *Trudy Instituta gosudarstva i prava RAN*. [Proceedings of the Institute of state and law], 2018. № 5. P. 117-149.

6. Ugolovnyi kodeks RF ot 13 iyunya № 63-FZ [Criminal code of the Russian Federation of June 13 № 63-FZ]. *Rossiiskaya gazeta ot 18 iyunya 1996 g. № 113, 114, 115, 118. [Rossiyskaya Gazeta of June 18], № 113, 114, 115, 118.*
7. FZ ot 6 aprelya 2011 g. № 63-FZ «Ob elektronnoi podpisi» [FZ of April 6, 2011 № 63-FZ "On electronic signature"], *Rossiiskaya gazeta ot 8 aprelya 2011 g. № 75 [Rossiyskaya Gazeta of April 8], 2011 № 75.*
8. FZ ot 27 iyulya 2006 g. N 149-FZ «Ob informatsii, informatizatsii i zashchite informatsii» [FZ of July 27, 2006 N 149-FZ "On information, Informatization and protection of information"] *Rossiiskaya gazeta ot 29 iyulya 2006 g. N 165 [Rossiyskaya Gazeta of July 29], 2006 N 165.*
9. Anderson C., Baskerville R.L., Kaul M. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems. Vol. 34, Issue 4, 2 October 2017, P. 1082-1112. DOI: 10.1080/07421222.2017.1394063.*
10. Baskerville R. Information security: Going digital (invited lecture). *Communications in Computer and Information Science. Vol. 963, 2019, P. 3-1447th. Annual Conference of the Southern African Computing Lecturers Association, SACLA 2018; Gordon's Bay; South Africa; 18 June 2018 do 20 June 2018. DOI: 10.1007/978-3-030-05813-5_1.*
11. Burukina O., Karpova, S., Koro, N. Ethical Problems of Introducing Artificial Intelligence into the Contemporary Society. *Advances in Intelligent Systems and Computing. Vol. 876, 2019, P. 640-6461. DOI: 10.1007/978-3-030-02053-8_98.*
12. Bouhadana I. *Ledroitairespectdelavieprivee a l'eredunumeriquedanslesystemefrancais. Evolyutsiya gosudarstvennykh i pravovykh institutov v usloviyakh razvitiya informatsionnogo obshchestva.. Moscow, 2012. P. 135-153.*
13. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunication sector. *OJ. L 24.Vol. 41. 30 January 1998. P. 1-8.*
14. Dneprovskaya N.V., Bayaskalanova, T.A., Ruposov, V.L., Shevtsova, I.V. Study of Digitization of Russian Higher Education as Basis for Smart Education. *Proceedings of the 2018 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 20185 November 2018, P. 607-6112018. IEEE International Conference ""Quality Management, Transport and Information Security, Information Technologies"", IT and QM and IS 2018; St. Petersburg; Russian Federation; 24 September 2018 do 28 September 2018. DOI: 10.1109/ITMQIS.2018.8524945.*
15. Frolova E.E., Polyakova, T.A., Dudin, M.N., Rusakova, E.P., Kucherenko, P.A. Information security of Russia in the digital economy: The economic and legal aspects. *Journal of Advanced Research in Law and Economics. Vol. 9, Issue 1, Spring 2018, P. 89-95. DOI: 10.14505/jarle.v9.1(31).12.*
16. Heaton, J., Parlikad, A.K. A conceptual framework for the alignment of infrastructure assets to citizen requirements within a Smart Cities framework. *Cities* Volume 90, July 2019, P. 32-41. DOI: 10.1016/j.cities.2019.01.041

17. Isa W.M.W., Zin, N.A.M., Rosdi, F., Sarim, H.M. Digital preservation of intangible cultural heritage. Indonesian Journal of Electrical Engineering and Computer Science. Vol. 12, Issue 3, December 2018, P. 1373-1379. DOI: 10.11591/ijeecs.v12.i3.pp1373-1379.
18. Jovanović M., Dlačić, J., Okanović, M. Digitalization and society's sustainable development — Measures and implications. Digitalizacija i održivi razvoj društva — Mjere i implikacije. Zbornik Radova Ekonomskog Fakultet au Rijeci. Vol. 36, Issue 2, December 2018, P. 905-928. DOI: 10.18045/zbefri.2018.2.905.
19. Mertens A., Schäfer, K., Rasche, P., Bröhl, C., Theis, S., Seinsch, T., Brandl, C., Wille, M. Shaping Ethical, Legal and Social Implications of the Digital Revolution Through Participation: The New Interdisciplinary Research Paradigm of Aachener DenkfabrEthik. Advances in Intelligent Systems and Computing. Vol. 824, 2019, P. 1493-1497 20th Congress of the International Ergonomics Association, IEA 2018; Florence; Italy; 26 August 2018 do 30 August 2018; Kod 216789. DOI: 10.1007/978-3-319-96071-5_152.
20. Pachis J.A., Zonneveld, K.L.M. Comparison of prompting procedures to teach internet skills to older adults. Journal of Applied Behavior Analysis. Vol. 52, Issue 1, Winter 2019, P. 173-187. DOI: 10.1002/jaba.519
21. Paillet L. Les ryeaux sociaux sur Internet et le droit au respect de la vie privye. Bruxelles, 2012. R. 19.
22. Sousa M.J., Rocha, Á. Digital learning: Developing skills for digital transformation of organizations. Future Generation Computer Systems. Vol. 91, February 2019, P. 327-334. DOI: 10.1016/j.future.2018.08.048.