ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ

Научная статья
УДК 342.9
EDN: HTPISS
doi: 10.21685/2307-9525-2024-12-1-4

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ (ОПЫТ КИТАЯ)

Владислав Георгиевич Романовский

Пензенский государственный университет, Пенза, Россия
up406@mail.ru

Аннотация. *Актуальность и цели*. Безопасность данных выступает условием нормального функционирования государства и общества. В условиях цифровизации всех аспектов коммуникационного взаимодействия обеспечение безопасности данных перестает быть частным делом их обладателя, перейдя в одну из центральных задач публичного управления. Основная цель исследования – определить особенности правового обеспечения безопасности данных, а с учетом значения компаративистики акцент сделан на изучении опыта Китайской Народной Республики. *Материалы и методы.* Эмпирическая база статьи включает в себя российские и зарубежные доктринальные источники (где приоритет отдан авторам из КНР), а также статистические данные об использовании цифровых технологий в мире. Использован сравнительно-правовой метод исследования, благодаря которому выделены основные положения Закона КНР 2021 г. о безопасности данных. *Результаты.* Подчеркивается необходимость государственной защиты прав граждан, одним из способов которой выступает введение собственного цифрового сегмента. Это привело к появлению специального термина «балканизация» Интернета, который получает свое распространение также на правовой режим данных. Обозначено, что поиск баланса – сложный путь, но именно благодаря ему возможен консенсус, который повлияет на международный обмен данными, их общую защиту при обработке и различном использовании. *Выводы.* Доказано, что цифровые данные в современном мире являются основой для выстраивания коммуникаций во всех сферах общественного взаимодействия. Цифровизация – тренд современного развития, которому подчиняются также процессы, происходящие в праве и государстве. Безопасность данных – это и условие нормального межличностного взаимодействия, и основа для построения глобальной цифровой экономики, и базис государственного управления. Особым примером построения национальной системы кибербезопасности является модель КНР, где в ее центре находятся такие ценности, как национальная безопасность и цифровой суверенитет.

Ключевые слова: данные, информация, цифровизация, цифровой суверенитет, КНР, государственное регулирование, безопасность

Для цитирования: Романовский В. Г. Правовое обеспечение безопасности данных (опыт Китая) // Электронный научный журнал «Наука. Общество. Государство». 2024. Т. 12, № 1. С. 32–41. doi: 10.21685/2307-9525-2024-12-1-4 EDN: HTPISS

PUBLIC LEGAL (STATE LEGAL) SCIENCES

Original article

LEGAL ENFORCEMENT OF DATA SECURITY (PRACTICES IN CHINA)

Vladislav G. Romanovsky

Penza State University, Penza, Russia

up406@mail.ru

Abstract. *Background*. Data security is a condition for the normal functioning of state and society. In the context of digitalization of all aspects of communication, ensuring data security ceases to be a private matter of its owner and holder, becoming one of the central tasks of public administration. The main goal of the study is to determine the features of legal support for data security, and taking into account the importance of comparative studies, the emphasis is placed on exploring the practices in the People's Republic of China. *Materials and methods*. The empirical base of the article includes the Russian and foreign doctrinal sources (where priority is given to the authors from the PRC), as well as statistical data on using digital technologies in the world. The comparative legal method is used, which enables highlighting the main provisions of the 2021 Data Security Law of the People's Republic of China. *Results.* The article emphasizes the need for state protection of citizens' rights, one of the ways of which is to introduce the national digital segment. This has led to the emergence of the special concept of the "Internet Balkanization", which also extends to the legal regime of data. The article indicates that finding a balance is a difficult path, but thanks to it the consensus is possible, which will affect the international exchange of data, their overall protection during processing and various use. *Conclusions*. The article proves that digital data in the modern world are the basis for building communications in all areas of public interaction. Digitalization is a trend of modern development, which also governs the processes taking place in law and state. Data security is both a condition for normal interpersonal interaction, a ground for building a global digital economy and a basis of public administration. The ultimate example of building a national cybersecurity system is the PRC model, which centers such values as national security and digital sovereignty.

Keywords: data, information, digitalization, digital sovereignty, People's Republic of China, government regulation, security

For citation: Romanovsky V.G. Legal Enforcement of Data Security (Practices in China). *Elektronnyy nauchnyy zhurnal "Nauka. Obshchestvo. Gosudarstvo" = Electronic scientific journal "Science. Society. State*". 2024;12(1):32–41. (In Russ.). doi: 10.21685/2307-9525-2024-12-1-4

Современный мир проходит новый этап трансформации, где одним из базовых аспектов становится цифровизация, затрагивающая практически все сферы индивидуальной и общественной жизни. Она стала настолько универсальной, что в научной литературе прилагательное «цифровая(-ой, -ое)» применяется к различным терминам: право, управление, экономика, государство. В основе инновационных информационно-коммуникационных технологий (ИКТ), отталкивающихся от цифрового кода, находятся данные. Это означает, что принципы функционирования информационного общества строятся на базе обмена данными. Не зря устойчивым становится высказывание: кровь современной экономики уже не нефть, а данные. Это относится и к иным процессам. Даже применение искусственного интеллекта возможно только в условиях формирования больших баз данных (что породило новое понятие – большие данные).

В Российской Федерации ключевым правовым актом, регулирующим информационные отношения, выступает Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Необходимо отметить, что одновременно с ним был принят еще один документ – Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», основная задача которого определить правовой режим данных, имеющих прямое или опосредованное отношение к конкретному физическому лицу [1].

Стремительное развитие ИКТ обусловливает модернизацию информационного права, что можно наблюдать по постоянным изменениям перечисленных выше законов, а также по введению экспериментальных правовых режимов. Иллюстрацией выступает Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"».

В таких условиях все больший приоритет отдается вопросам информационной безопасности. И если раньше защита персональных данных в основном выступала личным бременем (поскольку отсутствовали агрегаторы больших данных), то сейчас это один из вопросов национальной безопасности. Именно поэтому этот аспект является приоритетным для государства, озадаченного поиском новых средств и методов его обеспечения. Именно поэтому утечка данных не просто изъян в компьютерной системе, это элемент функционирования современных систем жизнеобеспечения. Обратим внимание, что федеральный проект «Информационная безопасность» включен в национальный проект «Цифровая экономика Российской Федерации» (его паспорт утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 апреля 2019 г. № 7) [2].

Указом Президента РФ от 5 декабря 2016 г. № 646 утверждена Доктрина информационной безопасности Российской Федерации, в которой отмечается, что ИКТ стали неотъемлемой частью всех сфер деятельности, приобрели глобальный характер, они обеспечивают реализацию стратегических национальных приоритетов. В Доктрине подчеркивается трансграничный характер ИКТ. Дополним, что основными технологическими гигантами, обеспечивающими функционирование ИКТ, выступают зарубежные IT-платформы, которые называют «глобальной четверкой» – GAMA (по первым буквам наименований) – Google, Amazon, Meta[1], Apple. Основные опасения заключаются в том, что все перечисленные компании агрегируют значительные объемы данных, охватывают своими услугами практически весь земной шар, самостоятельно определяют условия предоставления услуг, исходя из своих корпоративных интересов (зачастую открыто игнорируя национальные правила) [3]. Кроме того, указанные компании продвигают свой бизнес, нередко игнорируя национальные особенности, исходя из собственных корпоративных интересов. Это обусловливает особый подход к цифровым технологиям как гибридной угрозе [4], что позволяет рассматривать не только потенциальную пользу инноваций, но и вред, который могут нести в себе ИКТ.

В Доктрине информационной безопасности обозначены национальные интересы в информационной сфере, среди которых (на первом месте) обеспечение конституционных прав и свобод человека и гражданина. Содержится также дополнительное указание на получение информации и право на неприкосновенность частной жизни. Действительно, прямая связь оборота информации и защиты частной жизни давно отмечается в научных исследованиях. А. В. Преснякова проводит параллели с информационной открытостью, которая, безусловно, затрагивает и личные данные [5].

В науке предлагается формулирование нового права на информационное самоопределение [6]. Е. А. Миндрова [7], следуя этой логике, соотносит два смежных (по ее мнению) права – на доступ к информации и на неприкосновенность частной жизни. Причем доступ к информации необходим не только публичным институтам, но и самим гражданам для реализации своих иных основных прав и свобод. Например, для того, чтобы осуществить

[1] Организация, признанная в Российской Федерации экстремистской.

покупку недвижимости, необходимо быть уверенным в «чистоте» сделки, что невозможно обеспечить без доступа к реестру сделок.

Государственные информационные ресурсы наращивают свои объемы, а их создание происходит постоянно. Даже не имеющий юридического образования человек может назвать ГАС «Выборы», Единый государственный реестр недвижимости, Единый государственный реестр налогоплательщиков.

Многие заинтересованы в доступе к систематизированной информации, находящейся в указанных базах. Она имеет свою стоимость и весьма высокую. По анализу зарубежных источников цена одной утечки данных в 2022 г. составила 4,35 млн долл. США[1]. Если утечка касается реестров, где владельцем выступает гигант IT-индустрии или страна с большой численностью населения, то потенциальный ущерб может касаться значительной части всей нашей планеты. Например, утечка данных из компании «Alibaba» в июле 2022 г. затронула 1,1 млрд пользователей, из государственной базы Индии «Aadhaar» в марте 2018 г. – 1,1 млрд человек[2]. В Российской Федерации в 2023 г. Роскомнадзор зафиксировал 168 утечек персональных данных, из-за чего в открытый доступ попало более 300 млн записей[3].

Каждая такая утечка усиливает актуальность безопасности данных. Статья 3 Закона «Об информации, информационных технологиях и о защите информации» в числе принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации закрепляет обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации. Продолжением общего вектора на обеспечение безопасности можно считать Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (которая определяется через два ключевых понятия – состояние защищенности и устойчивое функционирование). Кроме того, следует упомянуть Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», который через защиту уязвимых лиц реализует общие принципы информационной безопасности. Анализируя правовые акты, направленные на обеспечение информационной безопасности в Российской Федерации, необходимо выделить следующие конкретные шаги:

– Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» закрепил общие принципы трансграничной передачи данных и соблюдения национальных интересов Российской Федерации при такой передаче;

– Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» определил российский сегмент сети Интернет, в рамках которого осуществляется деятельность государственных информационных систем;

– Указ Президента РФ от 12 апреля 2021 г. № 213 утвердил Основы государственной политики Российской Федерации в области международной информационной безопасности;

– Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» установил общие параметры цифрового суверенитета, нацеливая на создание собственной технологической основы ИКТ;

– Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» предусмотрел порядок реагирования на компьютерные атаки в отношении органов публичной власти;

[1] 130+ Data Breach Statistics 2024 – The Complete Look // Astra : website. URL: https://www.getastra.com/blog/security-audit/data-breach-statistics/ (дата обращения: 04.01.2024).

[2] Most significant cases of data breach worldwide as of August 2023 (in millions), by number of compromised data records and individuals impacted // Statista : website. URL: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/ (дата обращения: 04.01.2024).

[3] Утечки данных в России // TAdviser : сайт. URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных_в_России (дата обращения: 04.01.2024).

– Распоряжением Правительства РФ от 22 декабря 2022 г. № 4088-р утверждена Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации.

Приведенный перечень далеко не полный. Необходимо признать, что и правотворческий процесс в этом направлении не завершен, это актуализирует сравнительно-правовые исследования. С учетом специфики геополитической ситуации наибольший интерес вызывает опыт Китайской Народной Республики, уже давно реализующей практику информационной безопасности самого государства, опосредованно проецирующейся на всех граждан страны. Символом такой политики выступает проект «Золотой щит», который в иностранных источниках именуют «Великий китайский файрвол» [8]. Термин «Firewall» дословно переводится с английского как «противопожарная стена», но в настоящее время в эпоху ИКТ больше известен как программный (программно-аппаратный) элемент сети, ответственный за фильтрацию контента.

Сегментация Интернета, благодаря которой происходит попытка подчинения виртуального мира национальным правилам, получила особое наименование – балканизация [9], но есть и дополнительный термин «the Splinternet» [10]. Одной из причин такого явления выступает использование Интернета и ИКТ в противоправных целях (вплоть до ведения кибервойн [11]). Каждое государство защищает права своих граждан, и введение собственного цифрового сегмента – попытка противодействия возникающим угрозам. С другой стороны, наносится некоторый урон глобализации и свободному распространению информации. Именно поэтому поиск баланса – сложный путь, но именно благодаря ему возможен консенсус, который повлияет на международный обмен данными, их общую защиту при обработке и различном использовании. Нельзя не отметить, что с развитием ИКТ термин «балканизация» стал распространяться также на правовые режимы данных [12]. Цифровая экономика, будучи основным потребителем данных, в большей мере рассчитывает на свободный оборот информации. Однако абсолютизация принципа приводит к тотальным нарушениям, где отдельная личность – наименее защищенный субъект правоотношений. В то же время и сегментация Интернета не представляет собой значимую гарантию соблюдения конфиденциальности – жесткие системы регулирования уже показывали свою компьютерную уязвимость [13].

Китай, провозгласив принцип технологической независимости, проделал большой путь в этом направлении, сконцентрировав усилия на создании и продвижении инновационных продуктов. Так, мессенджер WeChat рекламируется не только как национальный продукт, но и как универсальное средство коммуникаций, которое может использоваться во всем мире. Аналогичным образом подаются социальные сети QQ и Sina Weibo. Если упоминать социальную сеть TikTok, то она давно уже составляет конкуренцию всемирно известным продуктам. Внедрение технологии 5G ассоциируется с китайской компанией «Huawei». Определенные преимущества различных инновационных продуктов заставляют страны проводить обновленные торговые войны, в рамках которых следование интересам национальной безопасности является условием введения ограничений. Ярким примером может служить политика США в отношении сети TikTok и продуктов компании «Huawei» [14].

Все указанные действия сочетаются с идеей цифрового суверенитета, на которой следует остановиться подробнее. В ее основе – распространение верховенства государства на все сферы юрисдикции, включая онлайн-пространство. Именно с такой трактовкой выступает лидер КНР Си Цзиньпин[1], а ее практическими элементами, отраженными в законодательстве КНР, являются «приземление» мировых технологических гигантов, в части локализации персональных и иных данных, а также производства ключевых элементов компьютерной техники на территории Китая; введение надзора за информационным пространством, включая фильтрацию контента с точки зрения соблюдения интересов национальной безопасности; накладывание ограничений на оборот криптовалют; поддержка национальных технологических гигантов [15].

[1] 中华人民共和国网络安全法 // 百度百科合作平台. URL: https://baike.baidu.com/item/中华人民共和国网络安全法/16843044?fr=aladdin (дата обращения: 05.01.2024).

Подобная политика наталкивается на уже существующие факторы, которые строят цифровой мир по иным канонам. ИКТ определяют такие признаки данных, как их мобильность, фрагментация и рассредоточенность, которые изначально затрудняют их «приземление» в пределах географического пространства. Кроме того, вся история саморегулирования Интернета минимизировала участие государств в глобальной системе управления данными. Ставка сделана на международные организации, транснациональные корпорации, отдельные технические группы, частные организации [16]. В этой части анализ потенциала Китая в цифровой экономике многими оценивается как сильно преувеличенный: для нее важны не сами данные, а их скорость и свобода распространения. С этими аспектами в КНР возникают искусственно созданные трудности [17].

В то же время КНР имеет значимые конкурентные преимущества. Если персональные данные считать «кровью» цифровой экономики, то нельзя забывать о численности населения – более полутора миллиардов, что создает дополнительные преференции. Кроме того, продвижение собственной IT-индустрии позволяет возместить те затраты, которые приходятся на обеспечение цифрового суверенитета, даже если это приводит к дублированию каких-то технологий [18]. Китай становится производителем больших данных, что способствует росту мировой цифровой экономики, в которой доля именно этой страны расширяется пропорционально производимым данным. В том числе, исходя из этого понимания, Китай внедряет различные цифровые новшества в системе управления, обгоняя в этом процессе многие индустриальные державы [19].

Учитывая специфику оборота данных и появление таких новых понятий, как «большие данные» и «открытые данные», в КНР пытаются совместить выгоду от глобализации, на принципах которой строится мировая современная экономика, и необходимость безопасности национального сегмента кибер-пространства. В этой части показательно мнение основателя компании «Huawei Technologies Co. Ltd» Жэнь Чжэнфэя: «Я считаю, что цифровая экономика должна быть глобальной. Поскольку границы ни одной страны не могут сдерживать развитие цифровой глобализации, тенденция цифровой экономической глобализации неудержима и не может быть разрушена. В будущем развитие информационного общества будет стремительно превосходить масштабы развития доиндустриального общества и идти быстрыми темпами»[1].

Дополним, что понимание цифровой глобализации обусловило подход «Huawei» к разработке программного обеспечения с открытым кодом. Это приведет к трансформации как самой компании «Huawei», так и ее партнеров. Предполагается, что это создаст инновационную экосистему, а доля цифровой экономики в КНР к 2025 г. достигнет 50 % ВВП[2].

В таких условиях на 29-м заседании Постоянного комитета Всекитайского собрания народных представителей 13-го созыва 10 июня 2021 г. принят Закон о безопасности данных. Он состоит из 7 глав, включающих 55 статей, вступил в силу с 1 сентября 2021 г. Закон представляет расширенное понимание данных – любая запись информации с помощью электронных средств. Это позволяет распространять его на метаданные, которые в современных условиях несут в себе значимую информационную нагрузку. Более того, для проведения интеллектуального анализа вполне достаточно метаданных, чтобы формулировать необходимые выводы для осуществления контроля за общественными процессами. Именно защита метаданных – одна из актуальных тем современных исследований, где нет единства мнений по поводу распространения на них общего режима защиты [20, 21].

В Законе постоянно проводится связь с защитой национального суверенитета и общественной безопасности. Статья 2 устанавливает экстерриториальную юрисдикцию для тех, кто хотя и осуществляет деятельность по обработке данных за пределами КНР, но «наносит ущерб национальной безопасности Китайской Народной Республики, общественным интересам

---

1 **与任正非咖啡**对话（第三期）：数字主权，从对话到行动 // 微博. URL: https://weibo.com/3626485974/If97V0DRy (дата обращения: 05.01.2024).

2 华为伙伴暨开发者大会2022：**跨**边界协同，共建新生态 // 计算杂谈网站. URL: http://www.jisuanzt.com/archives/1685.html (дата обращения: 05.01.2024).

или законным правам и интересам граждан и организаций». Одновременно провозглашается возможность ответных ограничений на вводимые другой страной дискриминационные меры против КНР в отношении инвестиций, торговли, связанных с данными и технологиями их использования и обработки (ст. 26).

Вся логика Закона выстроена вокруг соблюдения национальных интересов и национальной безопасности, что проявляется в следующих положениях:

– в общем требовании о приверженности общей концепции национальной безопасности (ст. 4);

– в обязанности всех субъектов при осуществлении деятельности по обработке данных не подвергать угрозе сферу национальной безопасности (ст. 8);

– в классификации и ранжировании всех данных, где один из ключевых критериев – национальная безопасность. Причем данные, имеющие отношение к национальной безопасности, являются основными национальными данными, в отношении которых вводится наиболее строгая система управления (ст. 21);

– в установлении государственной системы проверки безопасности данных, особенно тех, которые могут влиять на уровень национальной безопасности. Решения, принятые государственными органами в рамках реализации данных полномочий, являются окончательными (статья 24);

– во введении режима экспортного контроля в отношении данных, связанных с обеспечением интересов национальной безопасности (ст. 25).

– в закреплении повышенных штрафных санкций за нарушения законодательства об обороте данных при нанесении ущерба интересам национальной безопасности (гл. 6).

Обратим внимание также на следующие положения Закона о безопасности данных: 1) гарантирует свободный обмен данными (в качестве дополнения сделана ссылка, что это способствует развитию цифровой экономики); 2) закрепляет обязанность уважать общественную мораль и этику, соблюдать деловую и профессиональную этику, быть честным и заслуживающим доверия, брать на себя социальную ответственность в процессе обработки данных; 3) аккумулирует все усилия государства и общества для совместного поддержания безопасности данных (принцип солидарности распространяется также на помощь гражданам, которые имеют небольшие знания о цифровом мире); 4) вводит понятие больших данных (государство обязуется содействовать созданию инфраструктуры данных); 5) устанавливает обязательства государства по содействию построению электронного правительства; 6) формирует открытый каталог государственных данных (предусматривается понятие открытых платформ государственных данных – открытых данных).

Подведем итоги проведенного исследования.

Данные в современном мире являются основой для выстраивания коммуникаций во всех сферах общественного взаимодействия. Это придает им особое значение: политическое, экономическое, социальное. Одновременно данные – условие функционирования современных ИКТ. Таким образом, вопрос безопасности данных перестал быть частным делом их обладателя, перейдя в область публичного интереса.

Цифровизация – тренд современного развития, которому подчиняются также процессы, проходящие в праве и государстве. Цифровое право становится не просто новой отраслью системы, но и формой существования, в которой многие институты начинают функционировать по совершенно иным (отличающимся от традиционных) канонам.

Безопасность данных – это и условие нормального межличностного взаимодействия, и основа для построения глобальной цифровой экономики, и базис государственного управления. Исходя из значения кибербезопасности, различные государства пытаются выстроить собственную модель государственного регулирования. Особым примером выступает КНР, где в центре построения правового воздействия оказываются такие ценности, как национальная безопасность и цифровой суверенитет.

Список литературы

1. Гонтарь Л. О. О защите персональных данных как институте международной информационной кибербезопасности на примере проекции отдельных международных организаций // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 1 (80). С. 74–86. doi: 10.12737/jfld.2020.002 EDN: LTRZOU

2. Экономическое право : учебник / Н. Бондарь, Р. Амелин, Д. Артемова, Д. Велиева [и др.] ; под науч. ред. Н. С. Бондаря. М. : Проспект, 2021. 352 с. doi: 10.31085/9785392336791-2021-352 EDN: IYMONQ

3. Ghani N. A., Hamid S., Udzir N. I. Big Data and Data Protection: Issues with Purpose Limitation Principle // International Journal of Advances in Soft Computing an Its Application. 2016. Vol. 8, № 3. P. 116–121. URL: http://www.i-csrs.org/Volumes/ijasca/ID-40_Pg116-121_Big-Data-and-Data-Protection-Issues-with-Purpose-Limitation-Principle_2.pdf

4. Права человека и безопасность в современном мире: гибридные угрозы и новые вызовы : монография / Н. Н. Аверьянова, Д. С. Велиева, Е. А. Капитонова [и др.]. М. : Проспект, 2021. 152 с. EDN: QPDDNB

5. Преснякова А. В. Конституционное право на неприкосновенность частной жизни в условиях информатизации общества: современный зарубежный опыт : автореф. дис. … канд. юрид. наук : 12.00.02. М., 2010. 26 с. EDN: ZODCTL

6. Кучеренко А. В. Этапы и тенденции нормативно-правового регулирования оборота персональных данных в Российской Федерации // Информационное право. 2009. № 4. С. 32–37. EDN: KYMFUN

7. Миндрова Е. А. Коллизия права граждан на доступ к информации и права на неприкосновенность частной жизни в условиях информационного общества : автореф. дис. … канд. юрид. наук : 12.00.14. М., 2007. 31 с. EDN: NIQFWF

8. Cabestan J.-P. The State and Digital Society in China: Big Brother Xi is Watching You! // Issues & Studies. 2020. Vol. 56, № 1. doi: 10.1142/S1013251120400032

9. Hill J. F. A Balkanized Internet?: The Uncertain Future of Global Internet Standards // Georgetown Journal of International Affairs. International Engagement on Cyber 2012: Establishing Norms and Improving Security. 2012. P. 49–58. URL: https://www.jstor.org/stable/43134338

10. Lemley M. A. The Splinternet // Duke Law Journal. 2021. Vol. 70, № 6. P. 1397–1427. URL: https://law.stanford.edu/publications/the-splinternet/

11. Права человека и гибридные войны / А. В. Басова, Д. С. Велиева, Е. А. Капитонова [и др.]. М. : Проспект, 2023. 184 с. EDN: OYPXAR

12. Fernanda G. N., Pollicino O. The Balkanization of Data Privacy Regulation // West Virginia Law Review. 2020. Vol. 123, № 61. P. 61–115. URL: https://researchrepository.wvu.edu/wvlr/vol123/iss1/5/

13. Cate F. H., Kuner C., Millard C., Svantesson Dan Jerker B., Lynskey O. Internet Balkanization Gathers Pace: Is Privacy the Real Driver? // International Data Privacy Law. 2015. Vol. 5, № 1. doi: 10.1093/idpl/ipu032

14. Seiler J. T. TikTok, CFIUS, And The Splinternet // University of Miami International and Comparative Law Review. 2022. Vol. 29, № 2. Article 4. P. 36–61. URL: https://repository.law.miami.edu/umiclr/vol29/iss2/4/

15. 高奇琦. 数字革命中国家主权的建构 // 中国社会科学报. 2021. 2316期. URL: http://sscp.cssn.cn/xkpd/tbch/tebiecehuaneirong/202112/t20211224_5384895.html

16. Gu H. Data, Big Tech, and the New Concept of Sovereignty // Journal of Chinese Political Science. 2023. 3 May. doi: 10.1007/s11366-023-09855-1

17. Huang Y., Mayer M. Power in the Age of Datafication: Exploring China's Global Data Power // Journal of Chinese Political Science. 2023. Vol. 28, № 1. P. 25–49. doi: 10.1007/s11366-022-09816-0

18. 赵峰, 贺立龙. 规范和引导互联网平台资本健康发展 // 海派经济学. 2022. Vol. 20, № 2. P. 227–228. URL: https://d.wanfangdata.com.cn/periodical/hpjjx202202025

19. Mahoney J. G. China's Rise as an Advanced Technological Society and the Rise of Digital Orientalism // Journal of Chinese Political Science. 2023. Vol. 28. P. 1–24. doi: 10.1007/s11366-022-09817-z

20. Pandit H. J., O'Sullivan D., Lewis D. Queryable Provenance Metadata For GDPR Compliance // Procedia Computer Science. 2018. Vol. 137. P. 262–268. doi: 10.1016/j.procs.2018.09.026

21. Tzanou M. Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures // Journal of Internet Law. 2013. Vol. 17, № 3. P. 20–33. URL: https://ssrn.com/abstract=3076459

References

1. Gontar L.O. On Protection of Personal Data as an Idea of International Information Cybersecurity Using the Example of the Projection of Specific International Organizations. *Zhurnal zarubezhnogo zakonodatelstva i sravnitelnogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*. 2020;(1):74–86. (In Russ.). doi: 10.12737/jfld.2020.002
2. Bondar N., Amelin R., Artemova D., Velieva D. et al. *Ekonomicheskoe pravo: uchebnik = Economic Law: Textbook*. Moscow: Prospekt, 2021:352. (In Russ.). doi: 10.31085/9785392336791-2021-352
3. Ghani N.A., Hamid S., Udzir N.I. Big Data and Data Protection: Issues with Purpose Limitation Principle. *International Journal of Advances in Soft Computing and Its Application*. 2016;8(3):116–121. Available at: http://www.i-csrs.org/Volumes/ijasca/ID-40_Pg116-121_Big-Data-and-Data-Protection-Issues-with-Purpose-Limitation-Principle_2.pdf
4. Averyanova N.N., Velieva D.S., Kapitonova E.A. et al. *Prava cheloveka i bezopasnost v sovremennom mire: gibridnye ugrozy i novye vyzovy: monografiya = Human Rights and Security in the Modern World: Hybrid Threats and New Challenges: Monograph*. Moscow: Prospekt, 2021:152. (In Russ.)
5. Presnyakova A.V. *Constitutional Right to Privacy in the Context of Informatization of Society: Modern Foreign Practices*. PhD abstract. Moscow, 2010:26. (In Russ.)
6. Kucherenko A.V. Stages and Trends in Legal Regulation of Personal Data Processing in the Russian Federation. *Informatsionnoe parvo = Information Law*. 2009;(4):32–37. (In Russ.)
7. Mindrova E.A. *Conflict of Citizens' Right to Access Information and Right to Privacy in Information Society*. PhD abstract. Moscow, 2007:31. (In Russ.)
8. Cabestan J.-P. The State and Digital Society in China: Big Brother Xi is Watching You! *Issues & Studies*. 2020;56(1). doi: 10.1142/S1013251120400032
9. Hill J.F. A Balkanized Internet?: The Uncertain Future of Global Internet Standards. *Georgetown Journal of International Affairs. International Engagement on Cyber 2012: Establishing Norms and Improving Security*. 2012:49–58. Available at: https://www.jstor.org/stable/43134338
10. Lemley M.A. The Splinternet. *Duke Law Journal*. 2021;70(6):1397–1427. Available at: https://law.stanford.edu/publications/the-splinternet/
11. Basova A.V., Velieva D.S., Kapitonova E.A. et al. *Prava cheloveka i gibridnye voyny = Human Rights and Hybrid Wars*. Moscow: Prospekt, 2023:184. (In Russ.)
12. Fernanda G.N., Pollicino O. The Balkanization of Data Privacy Regulation. *West Virginia Law Review*. 2020;123(61):61–115. Available at: https://researchrepository.wvu.edu/wvlr/vol123/iss1/5/
13. Cate F.H., Kuner C., Millard C., Svantesson Dan Jerker B., Lynskey O. Internet Balkanization Gathers Pace: Is Privacy the Real Driver? *International Data Privacy Law*. 2015;5(1). doi: 10.1093/idpl/ipu032
14. Seiler J.T. TikTok, CFIUS, and The Splinternet. *University of Miami International and Comparative Law Review*. 2022;29(2 Article 4):36–61. Available at: https://repository.law.miami.edu/umiclr/vol29/iss2/4/
15. 高奇琦. 数字革命中国家主权的建构 // 中国社会科学报. 2021. 2316期. Available at: http://sscp.cssn.cn/xkpd/tbch/tebiecehuaneirong/202112/t20211224_5384895.html
16. Gu H. Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*. 2023;3 May. doi: 10.1007/s11366-023-09855-1
17. Huang Y., Mayer M. Power in the Age of Datafication: Exploring China's Global Data Power. *Journal of Chinese Political Science*. 2023;28(1):25–49. doi: 10.1007/s11366-022-09816-0
18. 赵峰, 贺立龙. 规范和引导互联网平台资本健康发展 // 海派经济学. 2022;20(2):227–228. Available at: https://d.wanfangdata.com.cn/periodical/hpjjx202202025
19. Mahoney J.G. China's Rise as an Advanced Technological Society and the Rise of Digital Orientalism. *Journal of Chinese Political Science*. 2023;28:1–24. doi: 10.1007/s11366-022-09817-z
20. Pandit H.J., O'Sullivan D., Lewis D. Queryable Provenance Metadata For GDPR Compliance. *Procedia Computer Science*. 2018;137:262–268. doi: 10.1016/j.procs.2018.09.026
21. Tzanou M. Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures. *Journal of Internet Law*. 2013;17(3):20–33. Available at: https://ssrn.com/abstract=3076459

Информация об авторе / Information about the author

В. Г. Романовский – кандидат юридических наук, доцент кафедры уголовного права, Пензенский государственный университет, 440026, г. Пенза, ул. Красная, 40.

V.G. Romanovsky – Candidate of Law, Associate Professor of the Department of Criminal Law, Penza State University, 40 Krasnaya street, Penza, 440026.

Автор заявляет об отсутствии конфликта интересов /
The author declares no conflict of interests

Поступила в редакцию / Received 12.01.2024
Поступила после рецензирования и доработки / Revised 10.02.2024
Принята к публикации / Accepted 28.02.2024