УДК 347.51
DOI: 10.17223/22253513/38/12

С.М. Зубарев, А.В. Травин, А.И. Фролов

ДЕЛИКТНАЯ ОТВЕТСТВЕННОСТЬ ПРИ ПРИНЯТИИ И РЕАЛИЗАЦИИ ГОСУДАРСТВЕННЫХ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ[1]

Проведен комплексный анализ условий деликтной ответственности публично-правовых образований за причинение вреда государственными управленческими решениями при эксплуатации государственных информационных систем, в частности особенностей ответственности при нарушении конфиденциальности и недостоверности данных информационных систем, а также нарушении идентификации и аутентификации. Кроме того, рассмотрена специфика деликтной ответственности агентов информационных систем, привлекаемых к эксплуатации информационной системы.
Ключевые слова: *деликт, государственная информационная система, цифровизация, государственное управленческое решение, агент информационной системы, гражданско-правовая ответственность.*

Безвредность управленческого решения не входит в общепризнанный специалистами в сфере административного права список условий эффективности государственного управленческого решения [1. С. 257–269; 2. С. 78–79]. Впрочем, и без подобного признания указанное свойство с уверенностью можно рассматривать в качестве обстоятельства, влияющего на эффективность управленческого решения в сфере государственного управления. Последствием нарушения рассматриваемого требования безвредности является не только констатация управленческого решения в качестве неэффективного, но гражданско-правовая ответственность публично-правовых образований за причинение вреда. Тем самым деликтная ответственность может рассматриваться как одно из последствий принятия неэффективного государственного управленческого решения и одновременно как средство повышения эффективности управленческих решений.

Общее учение о деликтной ответственности публично-правовых образований [3] пока оставляет в стороне представляющую научный интерес проблему поиска и анализа рисков наступления гражданско-правовой ответственности за причинение вреда государственным управленческим решением в условиях цифровизации. Вместе с тем управленческие решения, принимаемые и реализуемые с использованием цифровых государствен-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00749 «Механизм обеспечения эффективности государственных управленческих решений в условиях цифровизации».

ных информационных систем (далее – ГИС, ИС), обладают существенной спецификой, обусловленной механизмом принятия решений в условиях информационного взаимодействия, осуществляемого в цифровой форме, а также в условиях использования новейших цифровых технологий. Цифровые формы информационного взаимодействия предполагают хранение кодированной ЭВМ информации и передачу этой информации по сети ЭВМ.

1. Общие условия деликтной ответственности публично-правовых образований за причинение вреда государственными управленческими решениями при эксплуатации государственных информационных систем

При принятии и реализации государственных управленческих решений в цифровом формате используются различные ГИС, в том числе федеральные (ФГИС): государственная автоматизированная информационная система «Управление» (ГАС «Управление»), ФГИС «Единый портал государственных и муниципальных услуг (функций)»; «Федеральный реестр государственных и муниципальных услуг (функций)», «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». В ГИС интегрируются также ИС организаций, привлекаемых для осуществления публичных функций и при оказании государственных и муниципальных услуг.

При этом следует отметить расширяющийся функционал указанных систем. Так, в соответствии с Положением, утвержденным постановлением Правительства Российской Федерации от 25.12.2009 № 1088, ГАС «Управление» представляет собой единую распределенную государственную информационную систему, обеспечивающую формирование и обработку данных, содержащихся в государственных и муниципальных информационных ресурсах, данных официальной государственной статистики, сведений, необходимых для обеспечения поддержки принятия управленческих решений в сфере государственного управления, в том числе для информационного обеспечения стратегического планирования[1]

Принятие государственного управленческого решения с передачей соответствующей информации по сети (доведение до исполнителей, адресатов) создает угрозу несанкционированного доступа к информации, утечки информации, угрозу раскрытия персональных данных, чем может быть причинен ущерб охраняемым интересам граждан и организаций. Вполне реальна возможность причинения вреда управленческим решением при использовании ИС.

[1] О государственной автоматизированной информационной системе «Управление» : постановление Правительства РФ от 25.12.2009 № 1088. URL: https://base.garant.ru/197043/

Сформировалась судебная практика оспаривания бездействия органов власти, выражающегося в неисполнении обязанности по передаче в ГИС о государственных и муниципальных платежах сведений об оплате государственной пошлины[1] или уплате штрафов[2]. Отсутствие соответствующих сведений в указанной системе послужило основанием принятия органами власти вредоносных решений по принудительному взысканию уже оплаченных штрафов и об отказе в принятии должных управленческих решений.

Имущественный и неимущественный вред может быть причинен государством[3] в лице его органов и агентами, привлекаемыми государством для эксплуатации ИС (многофункциональные центры оказания государственных и муниципальных услуг (далее – МФЦ), удостоверяющие центры и другие организации) в следующих случаях: нарушение конфиденциальности данных, представленных в цифровом формате; недостоверность и неактуальность сведений, содержащихся в ГИС; риски, связанные с проведением электронной идентификации и аутентификации.

Статьей 1069 ГК РФ предусмотрена ответственность государства за вред, причиненный государственными органами и их должностными лицами в результате незаконных действий (бездействия) органов и должностных лиц, в том числе в результате издания акта, не соответствующего закону (иному правовому акту). Ответственность в силу этой статьи возлагается на государство, вред возмещается за счет казны. Может ли ст. 1069 ГК РФ применяться к случаям причинения вреда при получении третьими лицами несанкционированного доступа к информации об управленческом решении? Наступает ли ответственность государства в случае причинения вреда управленческим решением, если некорректное управленческое решение принято по причине компьютерной атаки, совершенной на сервер государственного органа, или при повреждении данных компьютерными вирусами?

Для ответа на поставленные вопросы необходимо выяснить применительно к теме исследования специфику условий гражданско-правовой ответственности (состава гражданского правонарушения): вреда, противоправности, причинно-следственной связи и вины.

Вред может выражаться в нарушении личных неимущественных прав (распространение персональных данных, распространение информации, не соответствующей действительности, в том числе порочащей честь и достоинство), в нарушении имущественных прав (повреждение или уничтожение имущества, причинение убытков, в том числе упущенной выгоды).

---

[1] Постановление Седьмого арбитражного апелляционного суда от 10.03.2015 № 07АП-680/15. URL: https://base.garant.ru/60602843/

[2] Постановление Арбитражного суда Дальневосточного округа от 28.10.2014 № Ф03-4928/14 по делу № А51-3848/2014; Постановление Арбитражного суда Дальневосточного округа от 02.09.2016 № Ф03-4041/16 по делу № А51-11999/2015; Кассационное определение СК по административным делам Пятого кассационного суда общей юрисдикции от 27.11.2019 по делу № 8а-44/2019. URL: https://www.garant.ru/

[3] Сформулированные в статье выводы применимы ко всем типам публично-правовых образований (РФ, ее субъектам, муниципальным образованиям).

Так, управленческое решение налогового органа об исключении субъекта малого предпринимательства из реестра субъектов малого и среднего предпринимательства может существенно ухудшить имущественное положение организации, лишив ее различных государственных преференций. Например, субъекты малого и среднего бизнеса, работающие в пострадавших от коронавируса отраслях, освобождены от уплаты налогов и взносов за II квартал 2020 г.

Противоправность выражается в нарушении норм объективного права в процессе принятия управленческого решения с использованием ГИС. В качестве противоправных следует рассматривать действия, причиняющие вред, но не само по себе возникновение убытков у потерпевшего. Противоправным действием следует считать управленческое решение, принятое при отсутствии на то материально-правовых оснований (в случае отказа в принятии решения – при их наличии). Если в соответствии с порядком принятия решения орган власти учитывает только сведения ИС, обладает ли принятое на основе некорректных сведений ИС решение признаком противоправности? Поиск ответа на поставленный вопрос необходимо производить с учетом присущего противоправности свойства объективности [4. С. 60–61]. Отказ в принятии решения, основанный на некорректных данных, содержащихся в ИС, при наличии материально-правовых оснований для принятия положительного решения следует рассматривать как деяние противоправное. При этом указанными материально-правовыми основаниями не являются процедурные или процессуальные (административно-правовые) аспекты принятия управленческого решения. Можно заключить при этом, что административно-правовая противоправность, обнаруживающая себя только в нарушении установленных процедур принятия управленческого решения, не равна гражданско-правовой противоправности, обнаруживающейся даже при принятии административно-правомерного решения по процедуре и форме, но при отсутствии гражданско-правовых материальных оснований.

Проблемой является установление причинно-следственной связи между убытками и управленческим решением. Формирование данных ИС осуществляется в рамках электронного взаимодействия. Но если соответствующие цифровые данные подверглись хакерской атаке или повреждены компьютерным вирусом? Можно ли утверждать, что причиной убытков послужило управленческое решение? Или же таковой причиной являются действия хакеров? Прямой непосредственной причиной причинения вреда является управленческое решение (а не действия хакеров), даже если такое решение принято на основе некорректных данных ИС или без учета данных, которые в нарушение установленных правил отсутствовали в ИС. Более того, нарушения требований к обеспечению надежности, защищенности, достоверности ИС сами по себе не являются юридически значимыми причинами возникновения вреда, поскольку являются косвенными причинами. Вместе с тем указанные причины подлежат учету при определении вины государства в совершении противоправного деяния.

Ключом к решению проблемы ответственности является вина государственного органа или должностного лица, принявшего управленческое решение, которая предопределена принципом виновной ответственности государства в соответствии со ст. 1069 ГК РФ. Можно ли поставить в вину органу публичной власти причинение убытков субъекту предпринимательской деятельности при указанных выше обстоятельствах? В гражданском праве под виной понимается отсутствие в действиях (бездействии) деликвента должной степени заботливости и осмотрительности, которая требовалась в конкретных условиях. Очевидно, что если органом власти – оператором ИС не предприняты должные меры по предотвращению компьютерных атак на свои серверы, следует констатировать наличие вины.

Поскольку на основании ст. 1069 ГК РФ наступает ответственность государства, а не конкретного органа власти, требования по принятию соответствующих мер заботливости и осмотрительности предъявляются ко всему государству. Это означает, что отсутствие возможности у конкретного органа власти противостоять компьютерным атакам не означает такое отсутствие у других органов государства, в том числе правоохранительных органов, служб обеспечения компьютерной безопасности. Сформулированный подход также разрешает проблему принятия управленческого решения одним органом власти (орган № 1) на основании данных ИС в условиях, когда ответственным оператором ИС является другой государственный орган (орган № 2), не принявший должных мер по обеспечению надлежащего функционирования ИС. Поскольку органы исполнительной власти являются частью государственного механизма, объективно противоправные действия органа № 1 и виновные действия органа № 2, взятые в совокупности, являются достаточными для возложения на государство гражданско-правовой ответственности за причинение вреда.

С учетом изложенного в большинстве случаев совершения компьютерных атак на ГИС, повреждений размещенных в них данных компьютерными вирусами можно ставить вопрос об ответственности государства за принятие вредоносного управленческого решения. Это составляет существенный правовой риск, связанный с принятием и реализацией государственного управленческого решения в условиях цифровизации.

1.1. Деликтная ответственность за нарушение конфиденциальности данных, представленных в цифровом формате

Гражданско-правовая ответственность государства может наступить в случае распространения конфиденциальных данных, представленных в цифровом формате, в частности персональных данных, сведений, составляющих охраняемую законом тайну (коммерческую, банковскую, налоговую, врачебную, нотариальную и т.д.).

Например, решением Якутского городского суда с казны Российской Федерации взыскана компенсация морального вреда, причиненного распространением инспектором ДПС персональных данных о гражданине,

содержащихся в ФИС ГИБДД-М. Решение оставлено в силе судом апелляционной инстанции[1].

В дополнение к указанным общим условиям гражданско-правовой ответственности целый ряд подзаконных актов конкретизирует требования по обеспечению защиты цифровых данных, хранящихся и передаваемых в ГИС. Так, Положением о единой системе межведомственного электронного взаимодействия, утвержденным постановлением Правительства Российской Федерации от 08.09.2010 № 697 (далее – Постановление Правительства № 697) предусмотрены требования по блокировке электронных сообщений и (или) ИС в случае выявления несанкционированных сеансов обмена сообщениями;, а также по защите передаваемой информации от несанкционированного доступа, ее искажения или блокирования[2].

Положение об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие ИС, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, утвержденное Постановлением Правительства Российской Федерации от 08.06.2011 № 451 (далее – Постановление Правительства РФ № 451), предусматривает требования по обеспечению гарантии целостности, подлинности, актуальности и безопасности информации. Пункт 11 Положения устанавливает обязанность операторов ИС органов и организаций по обеспечению защиты передаваемых сведений от неправомерного доступа, уничтожения, модификации, блокирования, копирования, распространения, иных неправомерных действий, а также по обеспечению соблюдения конфиденциальности информации ограниченного доступа.

Приказом Минкомсвязи России от 03.05.2014 № 120 определены требования к защите каналов связи средствами криптографической защиты информации, а также предусмотрено обязательное резервирование каналов связи.

Однако не следует рассматривать указанные и иные требования подзаконных актов по защите информации в качестве основных и тем более исчерпывающих при оценке виновности действий (бездействия), повлекших нарушение конфиденциальности информации. Приоритет имеют общие критерии вины, установленные гражданским законодательством, имеющим бóльшую юридическую силу.

Также следует отметить возрастающую актуальность проблемы конфиденциальности в связи с планами использования цифровых дублеров основных документов граждан в ИС в целях их презентации гражданином посредством проверки QR-кода в мобильном приложении[3].

---

[1] Апелляционное определение СК по гражданским делам Верховного Суда Республики Саха (Якутия) от 03.10.2018 по делу № 33-3524/2018. URL: http://www.garant.ru/

[2] Примечательно, что п. 8 указанного Положения содержит запрет на обработку в системе взаимодействия электронных сообщений, содержащих сведения, составляющие государственную тайну.

[3] В Минцифры допустили появление цифровых двойников документов россиян в 2021 году. URL: https://tass.ru/ekonomika/9895511

1.2. Деликтная ответственность при недостоверности и (или) неактуальности сведений, содержащихся в государственных информационных системах

Недостоверность и неактуальность сведений, получаемых с использованием ГИС, заключают в себе высокие потенциальные риски причинения вреда гражданам и организациям. Ряд ГИС затрагивает важнейшие для граждан и бизнеса сферы.

Так, суд удовлетворил иск собственника земельного участка к муниципалитету о возмещении убытков в размере утраты рыночной стоимости земельного участка в связи с невозможностью его использования по назначению по причине его расположения в охранной зоне газопровода[1]. Основанием возложения ответственности на муниципальное образование послужило его бездействие: невнесение сведений о газопроводе и его охранной зоне в информационную систему обеспечения градостроительной деятельности (ст.ст. 56, 57 Градостроительного кодекса РФ)[2].

В России действуют различные электронные ГИС. Например, ФГИС Единого государственного реестра недвижимости, которая заменила 340 разрозненных ранее существовавших ИС, обеспечивает регистрацию прав на недвижимость, предусматривает в перспективе получение выписок о правах от 30 секунд до нескольких минут[3]. В качестве ИС действуют банк данных, содержащий сведения, необходимые для осуществления задач по принудительному исполнению судебных актов, актов других органов и должностных лиц (ст. 6.1 Федерального закона от 02.10.2007 № 229-ФЗ «Об исполнительном производстве»), государственная информационная система о государственных и муниципальных платежах (ст. 21.3 Федерального закона от 27.06.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»; далее – Федеральный закон № 210-ФЗ) и др.

В соответствии с требованиями постановлений Правительства РФ № 697 и 451 органы и организации, участвующие в системе межведомственного взаимодействия, обеспечивают полноту и достоверность информации, содержащейся в электронных сообщениях, передаваемых с использованием системы взаимодействия, обеспечивают актуальность и достоверность хранимых в системе взаимодействия сведений.

Недостоверность и неактуальность сведений, содержащихся в ИС, может послужить основанием наступления гражданско-правовой ответственности государства при наличии всех соответствующих условий.

---

[1] Апелляционное определение судебной коллегии по гражданским делам Калининградского областного суда от 16.05.2017 № 33-2292/2017. URL: http://www.garant.ru/

[2] Указанная ИС ведется в электронной форме в соответствии с Постановлением Правительства РФ от 13.03.2020 № 279 «Об информационном обеспечении градостроительной деятельности».

[3] Виктория Абрамченко: В России ускорят регистрацию прав на недвижимость и запустят онлайн-сервис для получения сведений из ЕГРН. URL: http://government.ru/news/40723/

Юридически значимым применительно к ответственности обстоятельством является наличие или отсутствие свойства публичной достоверности данных ГИС. Указанное свойство означает, что добросовестный пользователь ГИС, полагающийся на содержащиеся в ней сведения, не несет неблагоприятных последствий недостоверности соответствующей информации. De lege ferenda следовало бы однозначно определить, какие ГИС обладают свойством публичной достоверности, а какие нет. При этом публичную достоверность целесообразно закрепить в качестве общего правила.

Сейчас только некоторые информационные expressis verbis обладают свойством публичной достоверности (Единый государственный реестр юридических лиц, Единый государственный реестр недвижимости). Публичная достоверность иных систем остается вопросом неопределенным. Так, один из арбитражных судов пришел к выводу, что общедоступная ИС об исполнительных производствах не обладает признаком публичной достоверности. По мнению суда, приложенный к заявлению скриншот страницы интернет-сайта не подтверждает отсутствия сведений об исполнительном производстве в базе данных исполнительных производств, поскольку информация может не выводиться (не находиться поисковым сервисом сайта) в связи с различными причинами (особенностями программы, техническими сбоями и др.)[1].

1.3. Деликтная ответственность при нарушении правил проведения электронной идентификации и (или) аутентификации

Требует внимания проблема распределения рисков наступления имущественного вреда, а также неблагоприятных последствий для неимущественной сферы пользователей государственных цифровых сервисов в случае использования чужого цифрового аккаунта (цифрового профиля). Решение указанной проблемы не может иметь универсального ответа и зависит от причин неверной идентификации (аутентификации).

Очевидно, что неблагоприятные последствия несанкционированного доступа к чужим данным несет лицо, сообщившее сведения о своих паролях или передавшее свои электронные ключи третьим лицам, равно как и не проявившее должной степени осторожности при их использовании, что сделало возможным несанкционированный доступ к данным для третьих лиц.

Так, на основании п. 13 Правил использования простой электронной подписи при оказании государственных и муниципальных услуг, утвержденных постановлением Правительства Российской Федерации от 25.01.2013 № 33, заявитель – владелец ключа обязан хранить в тайне ключ, принимать все возможные меры, предотвращающие нарушение его конфиденциальности. В силу п. 14 указанных Правил гражданско-правовую от-

[1] Постановление Пятнадцатого арбитражного апелляционного суда от 10.08.2020 № 15АП-7992/20 по делу № А32-53103/2019. URL: http://www.garant.ru/

ветственность за негативные последствия, наступившие в результате несоблюдения заявителем названной обязанности, несет заявитель.

В рамках единой системы идентификации и аутентификации предусмотрена возможность использования простой электронной подписи при условии, что при выдаче ключа простой электронной подписи личность заявителя удостоверялась на личном приеме (п. 2(1) Правил определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг, утвержденных Постановлением Правительства РФ от 25.06.2012 № 634). Выдачу ключа простой электронной подписи с обязательной проверкой личности заявителя производит оператор выдачи ключа (МФЦ и другие организации, участвующие в процессе оказания государственных и муниципальных услуг), который несет ответственность, если в процессе выдачи ключа допустил ошибку при установлении личности заявителя (п. 18 Правил использования простой электронной подписи).

В процессе принятия и реализации государственных управленческих решений используется также более сложный способ идентификации и аутентификации, предполагающий предварительное получение ключа квалифицированной электронной подписи. Выдачу ключей квалифицированной электронной подписи осуществляют аккредитованные удостоверяющие центры. При этом Правила использования усиленной квалифицированной электронной подписи при обращении за получением государственных и муниципальных услуг, утвержденные постановлением Правительства Российской Федерации от 25.08.2012 № 853, предусматривают обязательную проверку субъектом управленческого решения действительности квалифицированной подписи, с использованием которой подписан электронный документ (пакет электронных документов) о предоставлении услуги (п. 7).

В целях организации информационного взаимодействия органов власти с удостоверяющими центрами постановлением Правительства Российской Федерации от 22.12.2012 № 1382 введены в действие Правила присоединения к инфраструктуре взаимодействия информационных систем организаций, к которым, в частности, относятся аккредитованные удостоверяющие центры.

В качестве деликвента могут при наличии оснований выступать как удостоверяющие центры, допустившие нарушения процедур выдачи ключей квалифицированной электронной подписи, так и государство при причинении вреда его органами и должностными лицами.

К сожалению, государственная аккредитация удостоверяющих центров не является гарантией обеспечения законности. Так, с использованием фиктивной квалифицированной электронной подписи от имени гражданина и без его ведома в Москве было создано пять юридических лиц. Это обстоятельство послужило основанием иска. Суд апелляционной инстанции удовлетворил иск о признании недействительным заявления на изготовление сертификата ключа проверки усиленной электронной подписи, признании недействительными усиленной квалифицированной электронной подписи, сертификата ключа проверки усиленной электронной подписи.

Судом на основании данных экспертизы установлено, что личная подпись гражданина в документах о выдаче электронной подписи подделана[1]. Указанные случаи носят неединичный характер[2].

Поскольку неправомерно выданные ключи квалифицированной электронной подписи используются в целях получения государственных услуг, сформировалась судебная практика обжалования соответствующих действий и решений органов власти, в основном положительная[3].

Постановлением Правительства Российской Федерации от 28.11.2011 № 977 «О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"» утверждены Требования к единой системе идентификации и аутентификации. В частности, система должна обеспечивать защиту размещенной в ней информации в соответствии с законодательством РФ (п. 8 Требований).

Наблюдаемая тенденция по интеграции в особой электронной среде различных государственных услуг и сервисов по вопросам медицины, образования, жилищно-коммунального хозяйства, государственного и муниципального управления, доступ к которой осуществляется в рамках единой системы идентификации (аутентификации) только подчеркивает исключительную важность обеспечения корректной работы указанной системы. Это же обстоятельство увеличивает риски самого факта причинения вреда, равно как и является фактором, способствующим потенциальному увеличению размера вреда, причиненного государственным управленческим решением.

2. Деликтная ответственность, связанная с деятельностью агентов, привлекаемых к процессам принятия и реализации государственных управленческих решений с использованием государственных информационных систем

В работе ГИС принимают активное участие привлекаемые для этого в соответствии с требованиями нормативных правовых актов хозяйствующие субъекты, не обладающие статусом органа власти (многофункциональные центры оказания государственных и муниципальных услуг; аккредитованные удостоверяющие центры, выполняющие функции по со-

[1] Апелляционное определение Курского областного суда от 25.04.2019 по делу № 33-1186-2019. URL: https://oblsud--krs.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=23592527&delo_id=5&new=5&text_number=1

[2] Решение Калужского районного суда Калужской области от 17.01.2020 в рамках дела № 2-1-275/2020. URL: http://www.garant.ru/

[3] Постановление Девятого арбитражного апелляционного суда от 05.07.2019 № 09АП-59508/18; Постановление Девятого арбитражного апелляционного суда от 03.08.2020 № 09АП-22780/20 по делу № А40-286937/2019. URL: http://www.garant.ru/

зданию и выдаче сертификатов ключей проверки электронных подписей; оператор единой системы персональных и биометрических данных граждан – ПАО «Ростелеком»). Указанные и подобные хозяйствующие субъекты, привлекаемые органами государства для реализации функционала ГИС, можно условно именовать агентами ГИС.

Правила функционирования ГИС допускают известную самостоятельность агентов, например при проведении идентификации и аутентификации пользователей[1]. Все же в большинстве случаев управленческие решения принимаются органами государства. Роль агентов заключается в определенном содействии принятию решения. Агенты ГИС могут быть отнесены к инфраструктуре принятия государственных управленческих решений, поскольку функции указанных агентов являются вспомогательными.

В условиях взаимодействия субъектов принятия государственных управленческих решений с агентами, составляющими инфраструктуру принятия этих решений, приобретают очевидную актуальность по крайней мере два вопроса. Первый: имеются ли особенности гражданско-правовой ответственности государства за принятие вредоносных управленческих решений при содействии причинению вреда агентом ГИС? Второй: есть ли de lege lata и de lege ferenda основания субсидиарной ответственности публично-правового образования за вред, причиненный агентом ГИС?

2.1. Особенности гражданско-правовой ответственности государства за принятие вредоносных управленческих решений при содействии причинению вреда агентом информационной системы

На основании ч. 6 ст. 16 Федерального закона № 210-ФЗ вред, причиненный в результате ненадлежащего исполнения (неисполнения) возложенных на МФЦ обязанностей, возмещается в соответствии с законодательством РФ. Указанная отсылочная норма не позволяет однозначно определить субъекта гражданско-правовой ответственности за причинение вреда государственным управленческим решением, если причинению вреда содействовал МФЦ или иной агент ИС. Такое содействие может выражаться в искажении или потере данных, передаче неполных данных, нарушениях правил идентификации и аутентификации и т.д.

Деликтная ответственность государства за нарушение права частного лица вследствие принятия государственного управленческого решения может быть основана на нормах гражданского права при наличии условий гражданско-правовой ответственности за причинение вреда. Только одно из условий ответственности – вина субъекта принятия государственного управленческого решения – обладает значительной спецификой. О виновности свидетельствует непринятие мер по осуществлению контроля за со-

[1] Несмотря на свою дискуссионность, вопрос отнесения решений, принимаемых указанными агентами, к государственным управленческим решениям в настоящей работе не исследуется.

ответствующим агентом ГИС. Осуществление такого контроля следует рассматривать как обязанность государства в лице Минцифры России и других органов власти, являющихся операторами различных ГИС.

Следует подчеркнуть, что содействие агента ИС причинению вреда не исключает ответственности публично-правового образования. Принятие правомерного управленческого решения находится в сфере ответственности публично-правового образования, которое является деликвентом и возмещает противоправно причиненный управленческим решением вред.

Изложенный подход подтверждается судебной практикой. Так, суды признали незаконными действия налоговой службы, выразившиеся в совершении регистрационных действий (регистрация юридических лиц, изменение сведений в ЕГРЮЛ), несмотря на то что заявления о совершении регистрационных действий поданы с использованием фиктивных квалифицированных электронных подписей, выданных удостоверяющими центрами[1].

В другом деле суды отказали в иске к МФЦ, сотрудник которого принял неполный комплект документов и неверно ориентировал заявителя, что повлекло неблагоприятные для заявителя последствия: отказ в принятии решения о совершении регистрационных действий органом управления. При этом суд принял во внимание, что соответствующее решение принято органом власти, а не МФЦ[2].

По указанным соображениям невозможно наступление солидарной ответственности публично-правового образования (за неправомерное государственное управленческое решение) и агента ГИС (за содействие принятию подобного решения) на основании ст. 1080 ГК РФ за совместно причиненный вред. Надлежащим субъектом деликтной ответственности при принятии государственного управленческого решения является государство.

Однако это не устраняет возможности применения правила п. 2 ст. 1081 ГК РФ (о регрессе к лицам, совместно причинившим вред) по аналогии закона. Так, публично-правовое образование, возместившее вред, причиненный управленческим решением, вправе потребовать от агента ИС возмещения, соответствующего степени вины этого агента в общем объеме причиненного вреда.

2.2. Субсидиарная ответственность государства за вред, причиненный агентом информационной системы

Если вред не находится в причинной связи с действиями (бездействием) публично-правового образования или отсутствует вина такового, может

[1] Постановление Девятого арбитражного апелляционного суда от 05.07.2019 № 09АП-59508/18; Постановление Девятого арбитражного апелляционного суда от 03.08.2020 № 09АП-22780/20 по делу № А40-286937/2019. URL: http://www.garant.ru/

[2] Постановление Арбитражного суда Дальневосточного округа от 13.07.2017 № Ф03-2434/17 по делу № А51-20343/2016. URL: http://www.garant.ru/

наступать самостоятельная ответственность агентов ГИС: к примеру, если вред причинен распространением конфиденциальной информации агентом ГИС. Деликтоспособность агентов ГИС не вызывает сомнений, исходя как из общих начал гражданского законодательства, так из актов специального характера. На основании ч. 7 ст. 18 Федерального закона № 210-ФЗ МФЦ несет самостоятельную ответственность за вред, причиняемый привлекаемыми к оказанию государственных и муниципальных услуг организациями (с возможностью регрессного требования к таким организациям). Так, суд взыскал с МФЦ вред, причиненный утратой почтовой корреспонденции по вине почтовой организации[1].

С учетом роли агентов ГИС, привлекаемых к выполнению публичных функций, а также потенциально высокой вредоносности решений и действий указанных агентов резонным представляется вопрос о возможной субсидиарной ответственности государства за действия (бездействия) агентов ГИС.

В силу п. 5 ст. 2 Федерального закона № 210-ФЗ МФЦ имеют статус государственного или муниципального учреждения (в том числе автономного учреждения). При создании МФЦ в организационно-правовой форме казенного учреждения учредитель (субъект Российской Федерации или муниципальное образование) несет субсидиарную ответственность во всех случаях недостаточности имущества учреждения (п. 4 ст. 123.22 ГК РФ). За вред гражданам, причиненный МФЦ, созданным в форме бюджетного или автономного учреждения, учредитель несет субсидиарную ответственность (п.п. 5, 6 ст. 123.22 ГК РФ). Указанные нормы не решают проблему субсидиарной ответственности Российской Федерации за вред, причиненный МФЦ при содействии оказанию государственных услуг федеральными органами исполнительной власти.

Статья 1069 ГК РФ, устанавливающая ответственность публично-правового образования за вред, причиненный государственными органами, органами местного самоуправления, а также их должностными лицами, неприменима, поскольку МФЦ, удостоверяющие центры и другие агенты ГИС не являются органами государства.

Статья 403 ГК РФ об ответственности должника за действия третьих лиц, на которых было возложено исполнение обязательства, могла бы иметь шансы на применение по аналогии закона. Но, учитывая публично-правовую природу принятия и реализации государственного управленческого решения и выраженный в п. 3 ст. 2 ГК РФ запрет применения гражданского законодательства к публичным отношениям, норму ст. 403 ГК РФ не следует рассматривать в качестве применимой.

В практике Европейского суда по правам человека сложился подход, допускающий ответственность государства за деликты, совершенные юридическими лицами, на которые государством возложено осуществление

[1] Постановление Шестого арбитражного апелляционного суда от 04.07.2019 № 06АП-2951/19. URL: http://www.garant.ru/

публичных функций[1]. De lege ferenda такой подход следует развивать и в нашем праве.

Перспективные направления исследования

Исследовательский потенциал проблематика гражданско-правовой ответственности за причинение вреда в процессе принятия и реализации государственных управленческих решений имеет: при применении искусственного интеллекта (роботов); в автоматическом режиме («смарт решения»); на основе больших данных (big data).

Литература

1. Тихомиров Ю.А. Управленческое решение. М. : Наука, 1972. 286 с.

2. Ильченко Е.Н., Суркова С.А. Управленческое решение: разработка, принятие и реализация : учеб. пособие. Курган : Изд-во Курган. гос. ун-та, 2016. 124 с.

3. Кабанова И.Е. Гражданско-правовая ответственность публичных субъектов: вопросы теории и практики / отв. ред. М.А. Егорова. М. : Юстицинформ, 2018. 396 с.

4. Тархов В.А. Ответственность по советскому гражданскому праву. Саратов : Изд-во Саратов. ун-та, 1973. С. 60–61.

Zubarev Sergey M., Kutafin Moscow State Law University (Moscow, Russian Federation), *Travin Alexander V.*, St. Petersburg State Marine Technical University (Saint Petersburg, Russian Federation), *Frolov Aleksey I.*, Saint Petersburg Law School at the National Academy of General Prosecutor's Office (Saint Petersburg, Russian Federation)

TORT LIABILITY IN MAKING AND IMPLEMENTING PUBLIC MANAGEMENT DECISIONS USING DIGITAL INFORMATION SYSTEMS

Keywords: tort, government information system, digitalisation, government management decision, information system agent, civil liability.

DOI: 10.17223/22253513/38/12

The article provides a legal analysis of the conditions of civil liability for damage caused by the adoption and implementation of state management decisions taken during the operation of digital state information systems.

An approach to assessing the guilt of the state in taking a harmful management decision in the context of digitalization, consisting in the analysis of the actions of the entire state apparatus as a whole, rather than a single individual body that failed, for example, to resist computer attacks, is proposed.

The features of tort liability of the state for breach of confidentiality of digitally represented data and for harm caused by inaccurate (irrelevant) information of information systems have been considered. The principle of public reliability has been suggested as a general rule for state information systems. The opinion has been expressed that it is necessary to define unambiguously which information systems are characterized as publicly trustworthy.

The paper touches on the problem of tort liability in case of breach of electronic identification and authentication rules. The author has argued that both the certification centres which

[1] Постановление ЕСПЧ по делу «Костелло-Робертс против Соединенного Королевства» (Costello-Roberts v. United Kingdom) от 25 марта 1993 г., § 27, Series A, № 247; Постановление ЕСПЧ по делу «Ершова (Yershova) против Российской Федерации» от 8 апреля 2010 г. (жалоба N 1387/04) (Первая Секция).

violated the procedures of qualified electronic signature keys issue and public law entities when authorities and officials caused damage can be considered as a tortfeasor if there are reasons to do so.

An analysis was made of judicial practice of appealing against actions and decisions of public authorities taken on the basis of applications signed with fictitious qualified electronic signatures.

A special attention was paid to the tort liability associated with the activity of agents involved in the processes of adoption and implementation of state management decisions using information systems (MFC, certification centres etc.). Business entities contributing to the processes of information systems maintenance and engaged by the state bodies are suggested to be called "information systems agents".

The peculiarities of civil responsibility of the state for damage caused by a management decision promoted by an information system agent were considered. It was suggested to consider the state as a proper subject of tort liability, the guilt of which in this case was specific and consisted in failure to take measures for control over the corresponding agent.

The legal analysis of the grounds of vicarious liability of public-law entities for damage caused by information system agents was carried out. The opinion about independent liability of information system agent is argued if the harm is not in causal connection with actions (inactions) of public legal entity or if there is no guilt of public legal entity. On the basis of the practice of the European Court of Human Rights it is proposed de lege ferenda to fix the responsibility of the state for the torts committed by the persons entrusted by the state to perform public functions.

References

1. Tikhomirov, Yu.A. (1972) *Upravlencheskoe reshenie* [Management decision]. Moscow: Nauka.

2. Ilchenko, E.N. & Surkova, S.A. (2016) *Upravlencheskoe reshenie: razrabotka, prinyatie i realizatsiya* [Management decision: development, adoption and implementation]. Kurgan: Kurgan State University.

3. Kabanova, I.E. (2018) *Grazhdansko-pravovaya otvetstvennost' publichnykh sub"ektov: voprosy teorii i praktiki* [Civil liability of public entities: questions of theory and practice]. Moscow: Yustitsinform.

4. Tarkhov, V.A. (1973) *Otvetstvennost' po sovetskomu grazhdanskomu pravu* [Responsibility under the Soviet civil law]. Saratov: Saratov State University. pp. 60–61.